Business Continuity: *Plan…Train… Exercise*

Final Report

Prepared by

Participants of the
Georgia Digital Academy on
Business Continuity Planning

Prepared for

Robert Woodruff, Acting Director
Technology and Planning Division
Georgia Technology Authority
Atlanta, Georgia

Compiled and Edited by

Doris R. Konneh, Georgia Technology Authority
James Price, Georgia Technology Authority
Richard Halstead-Nussloch, Southern Polytechnic State University

February 2005

List of Figures

List of Tables

TABLE OF CONTENTS

EXECUTIVE SUMMARY

"I have always found that plans are useless, but planning is indispensable."
(General Dwight Eisenhower)

Business continuity refers to the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster or interruption. Not only does it aim to prevent the disruption of mission-critical services but also it attempts to fully re-establish those services as swiftly and smoothly as possible.

Participants

In the Georgia Digital Academy on Business Continuity Planning (GDBAC), over a period of thirteen weeks (September 14-15 and September 28-December 14, 2004), 87 representatives from 29 state agencies and sixteen subject matter experts from the state and federal government focused on business continuity/disaster recovery planning, preparation and practice for Georgia. *Table 1 and Table 2 provide a list of these participants, respectively*.

Senate Bill 243

Facilitated by Southern Polytechnic State University under the sponsorship of the Georgia Technology Authority, the intent of the GDABC was to help agencies become key players in developing safety plans. The requirement for such plans is in accordance with Senate Bill 243 (SB 243), which was signed into law by Governor Sonny Perdue in May 2004. *A copy of the bill is found in Appendix A*.

GDABC Deliverables

An overview of the primary deliverables from the GDABC follows:

- Ongoing briefings of agency and state executives on the progress of business continuity/disaster recovery planning activities
- Formulation of the first draft of a strategic, tactical and operational plan for business continuity for each agency
- Compilation of a GDABC report with recommendations on business continuity
- Initial assessment within pilot agencies of business continuity readiness based on results from the preparedness exercises, including recommendations for improvement
- Ongoing business continuity process education and internal consulting

- Ongoing development of a functioning, cross-agency business continuity team for Georgia
- Development of a resource plan to fund any business-continuity mandates beginning in FY07
- Development of the requirements for a RFP on business continuity
- Hosting of a business continuity/disaster recovery trade show

Overall Evaluation of the GDABC

At the conclusion of the GDBAC session, a Lickert scale was used to evaluate the sessions on nine factors. These factors are detailed in Appendix E. Overall, thirty-seven participants (85.6%) responded positively (either very satisfied or satisfied) on all the scales. That percentage increased to 95.8% when the neutral category was added to the satisfied category (in the graph below this is indicated by the % ~ Negative). Figure 1 shows the factor-by-factor results. They clearly indicate that the biggest challenge is teamwork followed closely by working statewide and sustaining effort for business continuity. Still, roughly 4 of every 5 participants are satisfied about the benefits to their agencies resulting from the GDABC.

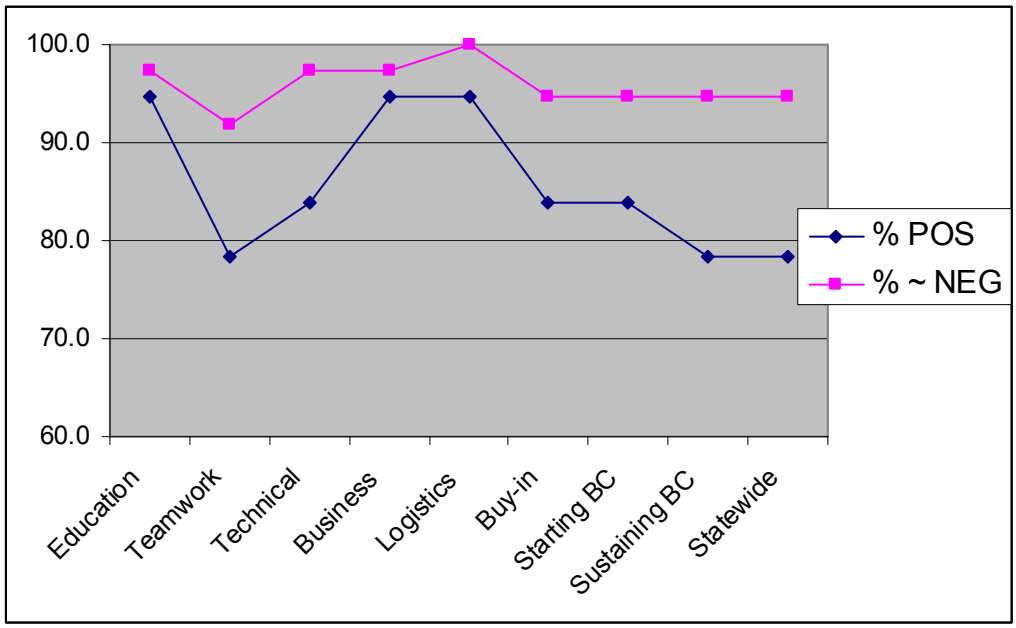

Figure 1. Results of GDABC Evaluation

Organization of the Final Report

This final report was compiled by the GDABC participants. Its body is organized into the following major sections:

1.0 INTRODUCTION - Description of the Georgia Digital Academy concept and an overview of the benefits resulting from the GDABC. It includes the following subsections:

1.1 Purpose - Major goals of the GDABC.

1.2 Benefits to Participants – Value derived from the GDABC.

1.3 Scope – Approach to business continuity/disaster recovery assumed by the GDABC, including a summary of specific activities undertaken.

1.4 Pertinent Legislation and Programs – Descriptions of current Federal and state statutes that are relevant to business continuity/disaster recovery.

1.5 GTA Policies, Standards and Guidelines – Description of the GTA process for the development of policies, standards and guidelines and how the work of the GDABC will be included in that process.

1.6 Major Issues in Business Continuity/Disaster Recovery - Description of the current "maturity" of agency business continuity/disaster recovery efforts.

1.7 Related Issues in Business Continuity/Disaster Recovery - Description of the need/acquisition of support for business continuity/disaster recovery at all levels both within the state and individual agencies.

2.0 METHODS AND PROCEDURES – Description of the overall design of the GDABC and the Fulmer approach to business continuity plan development. It includes the following subsections:

2.1 Major Structure – An overview of the setup of the GDABC.

2.2 Prominent Features – Description of the specific elements of the GDABC.

2.2.1 Fulmer Approach – Outline of the training curriculum used in the GDABC.

2.2.2 Boot Camp – Description of the contents of the preliminary initial training session that was conducted prior to the academy sessions.

2.2.3 SWOT Analysis – Description of the approach to examining the strengths, weaknesses, opportunities, and threats to business continuity faced by the GDABC participants' agencies.

2.2.4 Facilitated Interactive Sessions – Detailed description of the activities of each daily session.

2.2.5 Continuous Improvement and Web-based Research – Description of the use of WebCT, SPSU research assistants, and daily feedback/evaluation of sessions.

2.2.6 Subject Matter Experts (SMEs) – Description of the use of appropriate subject matter experts from across local, state, and Federal government agencies as needed.

2.2.7 Division into Communities of Interest – Description of division of participants into groups according to the type of service provided by their agency and per the category designations of the New Georgia Commission.

3.0 RESULTS AND DISCUSSION – Overall summary of the boot camp and daily sessions of the GDABC. It includes the following subsections:

3.1 Findings – Description of the overall findings of the GDABC regarding business continuity/disaster recovery, specifically strengths, weaknesses, opportunities, and threats and business continuity readiness/maturity.

3.1.1 Final SWOT Analysis – List of agencies' strengths, weaknesses, opportunities, and threats that may impact business continuity/disaster recovery planning as identified at the conclusion of the GDABC.

3.1.2 BC Maturity – List of the assessed business continuity/disaster recovery planning readiness of the agencies at the beginning and conclusion of the GDABC.

3.1.3 BC Plan Exercises – Description of the readiness of agencies to exercise ("test") their initial business continuity/disaster recovery plans during the first quarter of Fiscal Year 2005.

3.2 Recommendations – Description of how the individual agencies and the state (enterprise) may use the work of the GDABC in its business continuity/disaster recovery efforts immediately and in the future. The recommendations are categorized according to priority of implementation ("next steps").

3.2.1 Must Do - Suggested mandatory next steps that the agencies and state should execute in their business continuity/disaster recovery planning efforts.

3.2.2 Should Do - Suggested desirable next steps that the agencies and state should execute in their business continuity/disaster recovery planning efforts.

3.3 Formation of the GDABC Professional Association – Description of actions for 2005 to be taken by a users group composed of participants from the GDABC (and others) whose mission is to ensure continuous action in business continuity/disaster recovery.

3.4 Requests for Executives – Description of suggestions for how state executives can support the agencies in their ongoing business continuity/disaster recovery planning efforts.

4.0 REFERENCES AND BIBLIOGRAPHY – Resource materials that were used in the GDABC and other materials that may be used by agencies in their ongoing business continuity/disaster recovery.

5.0 APPENDICES – Documents that were used in the GDABC or that the participants recommend for future use, including a Glossary of Terms.

Table 1

GDABC Participants

AGENCIES
• Administrative Office of the Courts
• Department of Administrative Services
• Department of Agriculture
• Department of Audits and Accounts
• Department of Community Affairs
• Department of Community Health
• Department of Corrections
• Department of Defense
• Department of Education
• Department of Human Resources - Information Technology
• Department of Human Resources - Division of Aging Services
• Department of Human Resources - Office of Financial Services
• Department of Human Resources - Office of Investigative Services
• Department of Juvenile Justice
• Department of Law
• Department of Motor Vehicle Safety
• Department of Natural Resources
• Department of Technical and Adult Education
• Department of Transportation
• Georgia Bureau of Investigation
• Georgia Emergency Management Association
• Georgia Merit System
• Georgia Professional Standards Commission
• Georgia Public Broadcasting
• Georgia Technology Authority – Financial Systems
• Office of Planning and Budget
• Office of State Administrative Hearings
• Office of the Attorney General
• Office of Treasury and Fiscal Services
• Public Service Commission
• Secretary of State
• State Board of Workers' Compensation

Table 2

GDABC Participants

SUBJECT MATTER EXPERTS
• Department of Administrative Services – Risk Assessment
• Department of Technical and Adult Education – Facilities
• Georgia Building Authority
• Georgia Properties Commission
• Georgia Emergency Management Administration
• Georgia Secretary of State – Archives Division
• Georgia Technology Authority – Financial Services
• Occupational Safety & Health Administration
• University System of Georgia - Facilities

1.0 INTRODUCTION

The Georgia Digital Academy (GDA) is a prime catalyst for state agencies to come together to develop technical solutions to common business problems. A key initiative of the Georgia Technology Authority, the goals of the GDA are to:

- Facilitate collaboration and education among state agencies.
- Accelerate the identification and standardization of best practices throughout state government.
- Develop solutions to meet the business requirements of state agencies.

1.1 Purpose

The major goals of the GDABC were to:

- increase Georgia's capability for business continuity and preparedness for disasters and other interrupting events.
- facilitate, train and practice for compliance with the requirement of Senate Bill 243 for safety plans.

1.2 Benefits to Participants

The overall benefits that participants derived from the GDABC for 2004 are summarized as follows:

1. Developed an understanding of the concepts, terminology, methodology and realities of business continuity/disaster recovery preparedness.

2. Implemented an industry-accepted best practice (Fulmer) as the approach to business continuity/disaster recovery planning.

3. Learned from subject matter experts in business continuity/disaster recovery and related areas (e.g., risk assessment, risk management, business impact analysis, open records practices, and communications).

4. Teamed up across agencies and statewide to explore existing efforts in business continuity/disaster recovery planning.

5. Completed effective business continuity/disaster recovery preparations ("planning to plan") and plans for their "hometown" agencies.

1.3 Scope

The scope of the GDABC encompassed the development of a multi-agency approach to business continuity/disaster recovery planning via utilization of a step-by-step approach to plan development and implementation. In so doing, the academy addressed the agencies' overall goals of preserving capital and public trust, ability to serve constituents, and employee security/safety.

Specific activities that were undertaken and/or completed follow:

- Executive briefings covering progress on business continuity – ongoing (**Briefing deliverable**).
- Georgia business-continuity process education - "hold your hand through BC" – ongoing (**Education deliverable**).
- A functioning, cross-agency business-continuity team for Georgia – ongoing (**Team deliverable**).
- A first draft of a strategic, tactical and operational plan for business continuity for each agency, check-pointing scope with each agency (**Business Continuity Plan deliverable**).
- A GDABC report with recommendations on business continuity in Georgia (**Report deliverable**)
- An initial assessment within pilot agencies of business continuity readiness based on results from the preparedness exercises, including recommendations for improvement (**Exercise deliverable**)
- Resource plan to fund any business-continuity mandates beginning in FY07 (**Resource Plan deliverable**)
- Requirements for a RFP on business continuity (**RFP Requirements deliverable**)
- Business continuity and disaster recovery trade show (**Trade Show deliverable**)

1.4 Pertinent Legislation and Programs

The need for business continuity/disaster recovery planning encompasses all levels of government. These levels range encompass planning for continuation/resumption of services and functions at the national, state, and local government agency levels.

Homeland security is the top priority of government today; and in this information age business continuity planning/disaster recovery is among its major areas. Within this

context and environment, the GDABC first identified the individual agencies' own business continuity/disaster recovery planning needs. In the future, the participants will undertake the task of assessing and aligning these needs with those of the entire state (and the Federal government, where appropriate).

Senate Bill 243 is the major state legislation that was considered by the GDABC in its activities. In fact, this legislation served as the primary impetus for conducting the academy.

The major provisions of SB 243 include:

- requires state agencies to prepare a safety plan addressing the threat of terrorist attacks, natural disasters, hazardous materials, radiological accidents and "acts of violence."
- gives GEMA responsibility for establishing and maintaining a unified incident command system, training and certifying emergency response personnel.

1.5 GTA Policies, Standards, and Guidelines

The GTA has established a process for developing and implementing policies, standards and guidelines for IT statewide. With respect to business continuity/ disaster recovery planning, the multi-agency community of practice ("user group") resulting from this GDABC will recommend appropriate standards and best practices for consideration.

1.6 Major Issues in Business Continuity/ Disaster Recovery

At the initiation of the GDABC, two primary issues were evident:

1. Determination of the status of business continuity planning in the state agencies.

2. Assessment of the agency plan's compliance with the mandated safety plans of Senate Bill 243.

In September 2004, the development and administration of the *BC Maturity-Core Competency Questionnaire* by James Price, Business Continuity/Disaster Recovery Coordinator for GTA, revealed that Georgia was at the initial stages (termed *crawling* and/or *walking*) on all major aspects of business continuity planning. However, at the conclusion of the academy in December 2004, the follow-up administration of the Questionnaire revealed that the participating agencies had made significant progress on all major aspects of business continuity planning and were at the walking, walking and running, or running stages. (*See section 3.1.2 of this report for detailed results*.)

A copy of the BC Maturity-Core Competency Questionnaire is found in Appendix B.

At the conclusion of the academy in December 2004, a follow-up assessment revealed that the majority of the participating agencies had completed a first draft of a strategic, tactical, and operational plan for business continuity.

1.7 Related Issues in Business Continuity/ Disaster Recovery

The limited availability of resources (financial and human) was found to be the key impediment to the agencies' achievement of 100% compliance with mandated safety plans. For such compliance to become a reality:

- Continuity and safety planning and operations must become a top priority of agency executives.

- Funding and resource priorities must move toward an appropriate level. (Current benchmark industry estimates indicate that spending on disaster recovery range from 6-15% of the IT budget.)

2.0 METHODS AND PROCEDURES

The Georgia Digital Academy on Business Continuity was designed to ensure that participants receive maximum benefit from their attendance. Each session was one-half day (with the exception of two special full-day sessions) and was conveniently located in the training rooms of the Floyd Building in downtown Atlanta. This building is the home to numerous state agencies and is within close proximity of many others. Thus, agency representatives were able to participate in the academy and continue to fulfill their regular job responsibilities.

2.1 Major Structure

An overview of the major structure of the GDABC follows:

- Formalization of the need and value for BC planning and management in Georgia with adequate funding
- Early identification of BC experts for Steering Committee
- Initial training (boot camp) on BC for novices
- Expanded marketing and communication sessions
- Research support through SPSU
- Ongoing development of final report
- Special presentations in extended sessions
- Planned follow-on with BC Preparedness Drill
- Monthly executive briefings to state and agency executives, councils, and other stakeholders
- Formulation of an ongoing community of practice (user group)

2.2 Prominent Features

Participants invested a great deal of effort in the GDABC and can expect to receive maximum benefits from it. To meet these expectations, the academy used two primary techniques developed especially for adult instruction and collaborative problem solving: boot camp and facilitated interactive sessions. Both techniques utilized Fulmer's *Business Continuity Planning: a Step-by-Step Guide* as its training curriculum. The following sections present an overview of the Fulmer curriculum, boot camp, and facilitated sessions.

2.2.1 Fulmer Approach

After careful examination of a number of possible guides, James Price selected the guide by Kenneth Fulmer to use for the GDABC. The book and companion CD (of forms) provide a step-by-step approach to the monumental task of business continuity. It enabled the participants to move efficiently in understanding the theory, concepts, and practical application of the material to their particular agency plans. Also, it provided a flexible structure that can be expanded to accompany further development/refinement of plans as necessary.

An outline of the 12-step approach to business continuity planning proposed by Fulmer is found in the Table 3.

Table 3

Steps to Business Continuity Planning

1.	Writing the Purpose, Objectives, Scope and Assumptions
2.	Choosing Your Plan Coordinator and Development Team
3.	Assigning Action Items, Coordination Responsibilities and Time Frames
4.	Doing Your Risk Assessment
5.	Doing Your Business Impact Analysis
6.	Selecting Your Recovery Teams
7.	Developing Your Emergency Action Plans
8.	Selecting Vendors for Backup Processing and Other Services
9.	Writing Your Business Continuity Plan
10.	Testing Your Plan
11.	Distributing Your Plan
12.	Maintaining Your Plan

2.2.2 Boot Camp

From September 14-15, an intensive boot camp on business continuity/disaster recovery planning was conducted by Mike Wade, an adjunct professor from Southern Polytechnic State University. The primary goals of this endeavor were:

- To develop an understanding of the concepts, terminology, methodology and realities of BC / DR preparedness.

- To develop a “plan to develop a BC / DR Plan” that will satisfy agency needs (e.g., service levels and legislation).

- To develop a cost / benefit based model of risk and mitigation to promote objective, effective and efficient deployment of resources to improve BC / DR preparedness in Georgia.

An outline of the schedule for the boot camp is shown in Table 4:

Table 4

GDABC Boot Camp

Day 1	
8:30	Session 1 – Introduction to BC and DR
9:30	Session 2 – Steps to Develop a BC/DR Plan
10:30	15 Minute Break
10:45	Session 3 – Fulmer Steps 1, 2 and 3
11:45	1 Hour Lunch
12:45	Recap Morning Sessions
1:00	Session 4 – Fulmer Step 4: Assessing Risks
2:00	Session 5 – Fulmer Step 5: Impact Analysis
3:00	15 Minute Break
3:15	Session 6 – Fulmer Step 6: Recovery Teams
4:15	Wrap Up
4:30	Adjourn first day
Day 2	
8:30	Session 7 – Fulmer Step 7: Action Plans
9:30	Session 8 – Fulmer Step 8: Alternate Locations
10:30	15 Minute Break
10:45	Session 9 – Fulmer Step 9: Writing the Plan
11:45	1 Hour Lunch
12:45	Morning Recap
1:00	Session 10 – Fulmer Step 10: Testing the Plan
2:00	Session 11 – Fulmer Step 11: Plan Distribution
3:00	15 Minute Break
3:15	Session 12 – Fulmer Step 12: Plan Maintenance
4:15	Wrap Up
4:30	Adjourn

2.2.3 SWOT Analysis

Utilizing the procedure recommended by the Management Sciences for Health and the United Nations Children's Fund, the GDABC participants completed an initial analysis of strengths, weaknesses, opportunities and threats, commonly known as a SWOT. (*See http://erc.msh.org/quality/ittools/itswot.cfm*). In this analysis, they identified their agency's internal resources and capabilities supporting business continuity as strengths and those factors inside their agency that represented an absence of a strength as weaknesses. Also, within the environment outside their agency, participants identified opportunities for growth and synergy of the agency's resources and capabilities for business continuity. Threats to the business-continuity capability from outside the agency were the final items identified. (*Further definition of SWOT is available at http://www.quickmba.com/strategy/swot/*.)

2.2.4 Facilitated Interactive Sessions

People often learn best when interacting with each other and actively practicing new skills. Although state agencies have widely varying roles and responsibilities, they face many of the same challenges in using IT to meet their business needs.

The GDABC used facilitated interactive sessions that were structured around both individual breakout groups and whole group activities. Each session began with the review of an agenda for the day and culminated with an evaluation of the day's activities. In addition, minutes were recorded of each session and provided to the participants via WebCT, an online Web-based discussion repository administered by SPSU.

A general outline for the facilitated interactive sessions is found in Table 5. For a complete set of agendas and the corresponding minutes for each session, see Appendix C.

Table 5

Outline of Facilitated Interactive Sessions

• Opening Plenary Session
– Status briefing and agenda for week
– Presentation to overview pertinent GTA standards, policies, procedures and specific tasks and GDABC goals on topic
• Facilitated breakout group work on topic
– Review/refine input from GTA, CIO Council, industry, etc.
– Draft recommendations for GDABC action
• Facilitated whole group work on topic
– Review/refine breakout group input
– Draft recommendations to GTA and other stakeholders

2.2. 5 Continuous Improvement and Web-based Research

Information technology standards and best practices are changing rapidly. To help participants keep up with these changes, the academy emphasized continuous improvement—that is, *learning to learn*. Members of the GDABC were allowed to avail themselves of information from the best sources on the Web and elsewhere. This research was conducted by SPSU graduate assistants who investigated issues and domains of interest to the participants and mined BLOGs.

Some of the more pertinent information resulting from the Web-based research appears in Appendix D.

Ongoing feedback was collected after each session. This feedback allowed the GDABC facilitators and staff to tune the sessions to meet the needs of the greatest number of participants. The final evaluation and feedback form is contained in Appendix E.

2.2.6 Subject Matter Experts (SMEs)

The GDABC hosted select experts and implementers of business continuity/disaster recovery planning and related areas. Participants met and worked with these SMEs and consultants, heard firsthand accounts from organizations with experience in the areas of interest identified by the agencies and staff of the academy, and posed questions regarding their respective areas. (*See Table 2 for a complete list of the agencies that served as subject matter experts*.)

2.2. 7 Division into Communities of Interest

The number and the diversity of participants suggested division into breakout groups for active discussion and development/modification of the draft business continuity/disaster recovery plans. The initial division was based upon voluntary selection into groups.

Subsequently, upon the suggestion of Robert Woodruff of GTA, the agencies were reorganized to adhere to the category designations of the New Georgia Commission to facilitate cross-agency work. (*See http://www.gov.state.ga.us/commission_newga.shtml*).

The final division was as follows:

- Administration/Financial
- Education
- Legal/Regulatory
- Safe/Safer Georgia

The academy staff of the Georgia Technology Authority divided their attention among the groups during the breakout sessions.

3.0 RESULTS AND DISCUSSION

This section provides an overall summary of the boot camp and daily sessions of the GDABC. It contains certain key findings as well as recommendations for further action by agency and state executives and other personnel.

3.1 Findings

Two of the major outcomes of the GDABC were findings related to the agencies' (1) overall strengths, weaknesses, opportunities, and threats (SWOT) and (2) readiness/maturity in the areas of business continuity/disaster recovery planning.

3.1.1 Final SWOT Analysis

The results of a SWOT conducted during the first daily session of the academy were used as the basis for structuring many of the ensuing discussions for the remainder of the GDABC:

Strengths
(an agency's internal resources and capabilities supporting business continuity)

- Facility locations (single or multiple, geographic distribution, regional)
- Contingent facilities, physical location, different locations available
- Controlled/secure facilities
- Technology resources – personnel, hardware, IT departments, GTA
- Military readiness
- Redundant systems / multiple locations
- Centralized planning, IT centrally managed and operated, good internal control
- All employees in a single location
- Decentralized implementation and execution
- Awareness of BC, awareness of need of BC
- Automation (UPS, generator, water supply)
- Outsourced resources with disaster recovery plan (health benefits, claims, etc.)
- Relationships with suppliers, regulatory agencies & key agencies
- Good paper fallback
- Self supported infrastructure

Weaknesses
(factors inside an agency that represent the absence of a strength)

- Budget, financial, lack of funding
- Stretched personnel resources, staff turnover
- Executive understanding of BC, limited business users' / executive understanding

- Lack of enterprise approach, lack of top-level support
- Lack of communication, lack of knowledge transfer
- Employee awareness and training (weak or non-existent)
- Physical location, multiple facility locations, too much redundancy
- Limited mitigation – Centralization, All employees in a single location
- Stakeholder commitment, lack of follow through, customer / consumer issues
- Single point of failure, no mainframe backup – state data center
- Dependence on other agencies, reliance on other agencies,
- Dependence on IT department
- No off-site storage facilities
- Technology not easily duplicated
- Paper
- False sense of security
- Out-of-date plan, Clear ID of needs missing (i.e., critical vs. essential)

Opportunities
(within the environment outside an agency, opportunities for growth and synergy of the agency's resources and capabilities for business continuity)

- Digital Academy, DA provides opportunity for personnel buy-in
- GTA, assistance from BGA/GTA to avoid duplicate effort
- Consolidate and coordinate multiple plans
- Collaboration among agencies, resource sharing, Ability to share with others
- Identify areas to share resources, Info / process sharing
- State/federal partnerships
- Cross training, training within key roles, education for the leadership team
- Educate tenants of IT resources
- Emerging technology (i.e., MPLS)
- Leverage support from private sector business partners (+) and media (+-)
- Have attention of agency heads after Ivan / power outage

Threats
(threats to the business-continuity from outside the agency)

- Cost, resources – ability to fund plan and updates, competition for resources
- Politics, political environment (federal and state level), sell-ability
- Terrorism, bioterrorism, hazardous materials
- Terrorist (train in building), terrorists – physical, cyber, LT
- Technology threats, technology-dependant threats, viruses
- Internal operations, Service-Level agreements, facility age / maintenance
- Weather, acts of nature, power outage, fire
- Media – unfettered, uncontrolled
- Disgruntled employees, outside vendors
- Duration / severity
- GBA (landlord relationships)
- Perceived need

The SWOT factors were prioritized by the GDABC participants. Figure 2 shows the results for the strengths, indicating that Georgia's technology resources including the GTA is seen as the major strength for business continuity. Figure 3 shows the results for the weaknesses. There is no surprise at budget being identified as the top weakness. Figure 4 shows the results for opportunities clearly indicating that assistance from statewide agencies and cross-agency teamwork were seen as the greatest opportunities. Figure 5 shows the results for threats where costs and the competition for resources are seen as the greatest threats to Georgia's business continuity.

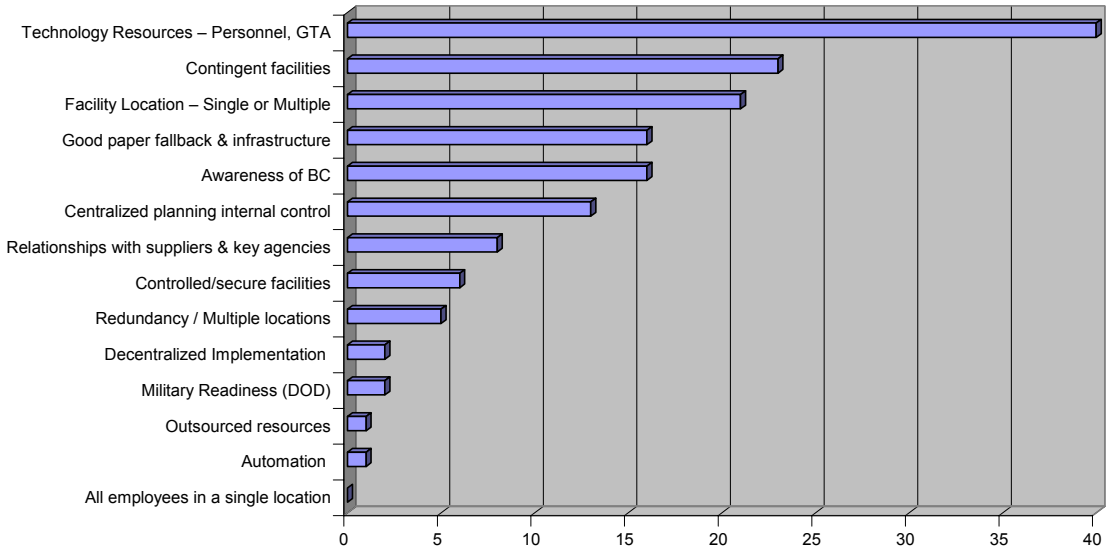

Figure 2. Strengths as prioritized by the GDABC.

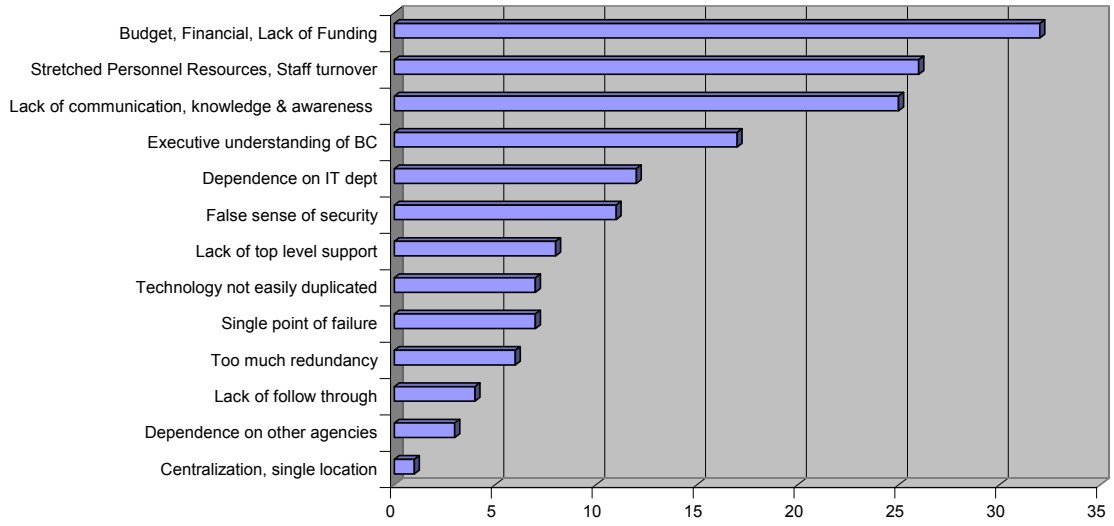

Figure 3. Weaknesses as prioritized by the GDABC

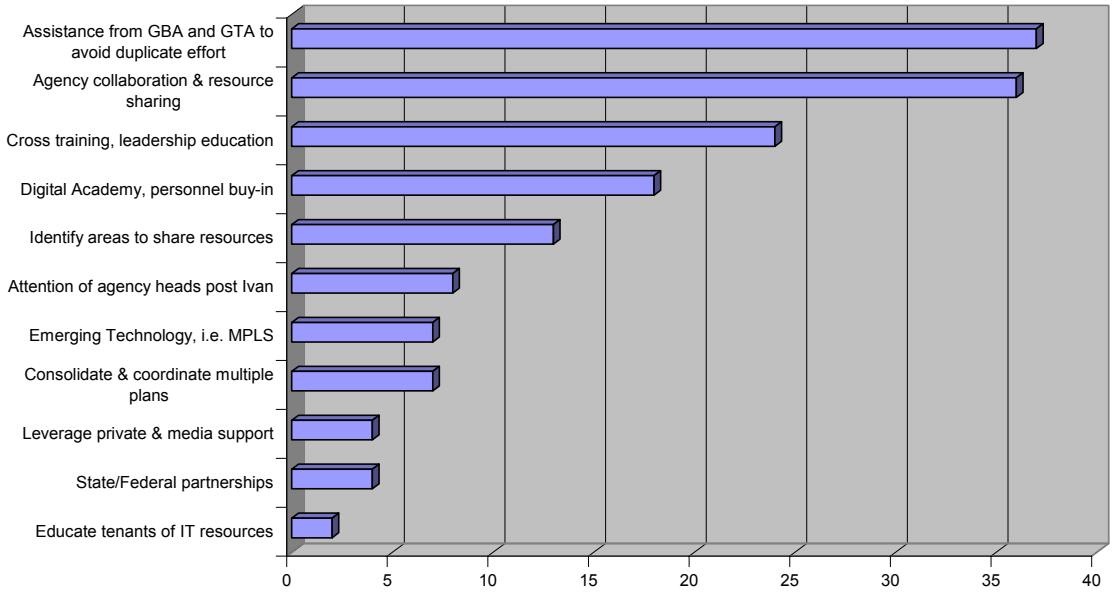

Figure 4. Opportunities as prioritized by the GDABC

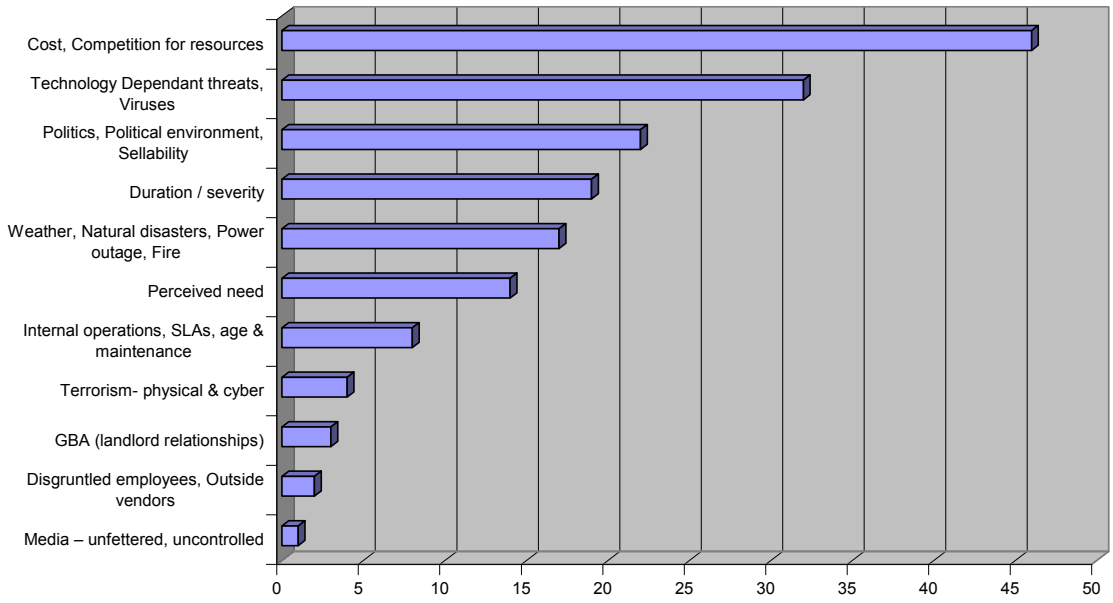

Figure 5. Threats as prioritized by the GDABC

The participants identified the following as the most critical of the **internal weaknesses and external threats**:

- Lack of funding and competition for resources
- Stretched personnel resources and personnel turnover
- Lack of communication, knowledge and awareness at all levels within the agencies
- Dependence on technology that is subject to physical and cyber threats

The participants identified the following as the most critical of the **internal strengths and external opportunities**:

- Assistance from GTA, GBA and GEMA to avoid duplication of effort
- Collaboration and shared resources among agencies
- Cross-training and leadership education, e.g., the Georgia Digital Academy
- Strong technology resources and personnel, both centralized and decentralized

The SWOT analysis proved useful throughout the GDABC to provide a sharp focus on the factors that were most important.

3.1.2 BC Maturity

The findings generated by administration of the revealed significant progress in this area as evidenced by the following results:

Business Continuity Maturity of Agencies
(September 2004)

Crawling	**Walking**
Measuring Performance (metrics)	Pervasiveness
Employee Awareness	BC Program Structure
Resource Commitment	External Coordination
	Leadership

Business Continuity Maturity of Agencies
(December 2004—Dot Vote)

Crawling
None

Walking
- Leadership
- Pervasiveness
- Measuring performance (metrics) (+1)
- Resource Commitment (+1)

Walking and Running
- BC Program Structure (+1)
- External Coordination (+1)

Running
- Employee Awareness (+2)

Figure 6 shows the results that the participants submitted during the last session of the academy on December 14, 2004 (n=36). They are comparable to the dot vote results and clearly indicate that the GDABC improved the maturity level of participating agencies and Georgia state government.

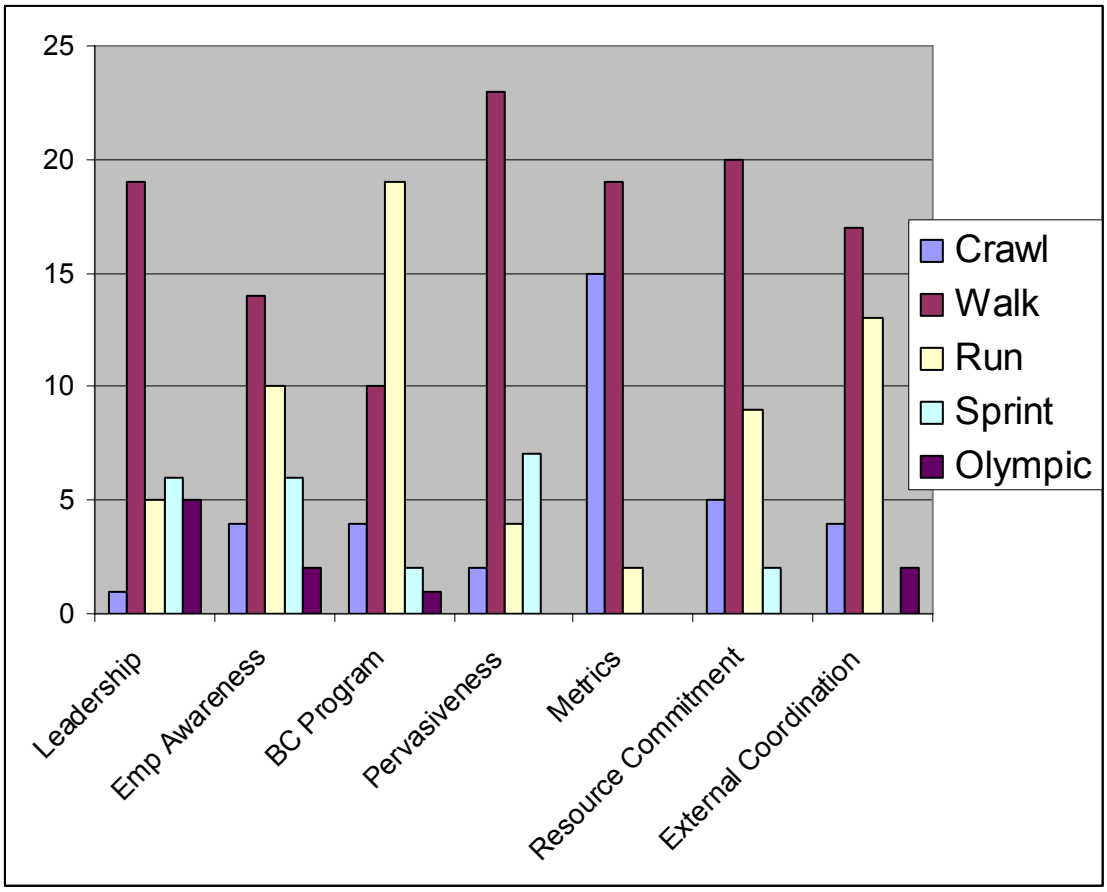

Figure 6. Business Continuity Planning Maturity Status

Twenty-two of the twenty-six reporting agencies (85%) had completed an extended outline or more of their agency's business continuity plan. Fifteen of the twenty-six (58%) reported significant progress toward obtaining executive support of business continuity in their agencies. The fact that not all agencies have completed the outline of their plans appears related to the lack of executive support. To increase the number and percentage of agencies with plans will likely require more executive support.

Table 6 shows the percentage of forty-five GDABC participants who indicated that their business continuity plan would contain a specific feature. Almost three-quarters of the respondents indicated their plan was built to address a worst-case scenario. This was a recommendation of both Fulmer and many of the subject matter experts. Over one-half of the participants indicated a change in funding priorities or additional funding was required to effectively put business continuity in place in their agency. About two in five of the respondents indicated their plans relied upon external vendors and partnerships with other state agencies. About one in five said their plan had common areas with other state agencies. Overall, the plans appear to be following best practices, make use of commonalties and partnerships, but will require changing funding priorities and/or additional funding to make Georgia fully ready.

Table 6

Percentage of Plans with Specific Feature

Percentage	Plan Feature
71%	Address a worst-case scenario
53%	Requires changing funding priorities or additional funds to put business continuity in place
42%	Relies on external vendors
42%	Relies on other state agencies
20%	Includes areas in common with other state agencies

3.1.3 BC Plan Exercises

Table 7 shows the percentage of forty-five GDABC participants who responded to questions about their desired level of participation in the exercise of the business continuity plans that was planned for the first half of 2005. This table shows that about two-thirds of the respondents want to be kept informed of the exercise status. About one-half want to observe another agency's exercise. About one-third wants to exercise their agency's plan and about one in five wants to help with the exercise in another agency. It appears from this data that the overall planning of this digital academy met the mark in that it provides for academy personnel to perform the staff work of the exercise.

Table 7

Percentage of Plans for Exercises

Percentage	Level of Participation in the Exercise
64%	Obtain a briefing and report on the exercise
49%	Observe another agency as that plan is exercised
31%	Exercise their agency's BCP
18%	Help in the exercise of another agency's BCP

3.2 Recommendations

The following sections describe how the individual agencies and the state (enterprise) may use the work of the GDABC in its business continuity/disaster recovery efforts immediately and in the future. They are categorized as *Must Do* and *Should Do* to indicate priority.

3.2.1 Must Do

- actions should be taken within individual agencies and statewide to effectively plan, prepare, budget, practice, improve and operate for business continuity
- agencies must share the responsibilities and resources required for business continuity
- agencies need adequate funding for business continuity activities
- preservation of life and safety must be the top priority of all business continuity planning

- On an ongoing basis, adequate funding and continuous exercising and improvement is required for all continuity planning and action.

- Because continuity planning and actions represent a large and major endeavor, agencies must share the burden and the resources required to meet it. Through communication, sharing and joint action, the overwhelming nature of continuity can be managed. Specific areas for sharing include:
  - Shared recovery facilities and resources including shared Hot Sites for 24/7/365 continuity of life-critical functions
  - Utilization of statewide resources, e.g., DTAE and USG schools and their assets, GBA, GEMA, GTA and their assets and processes
  - Negotiated assistance agreements with other states or the Federal government

- In addition to each agency taking action, actions should be taken statewide to effectively plan, prepare, budget and operate for continuity. Specifically,
  - The Governor should appoint a statewide Continuity Coordinator to facilitate and coordinate communications, planning, budgeting, exercises, etc. for continuity.
  - The Governor and/or Legislature should request a status report of each Agency's Business Continuity or Safety Plan on an annual basis.
  - Relevant statewide agencies and authorities, such as GBA, GEMA, GTA, DOAS Risk Management, OPB and others deemed appropriate should review and appropriately update processes and criteria pertaining to continuity and the safety plans.
  - Continuity should be brought up to the enterprise level by appropriately

    - Building a coherent continuity program by leveraging the Statewide Enterprise Architecture and *vice versa*
    - Developing an enterprise approach for procurement and evaluation of products and services for recovery and continuity
    - Bridging between continuity approaches and Team Georgia

- In all continuity planning and implementation, people should come first. Specifically, this means that
    - Preservation of life and safety must be placed at the top priority of all continuity planning and operations as well as the care and comfort of employees (and their families too) during recovery periods...
    - Coordination and communication with first-responders needs coverage and practice.
    - A critical mass, if not all state employees, should be trained in the fundamentals of first aid.
    - Steps should be taken to ensure that as many employees as possible receive (some) compensation during recovery periods where they can not work.
    - Evacuation and/or sheltering-in-place should be drilled and practiced.
    - Each set of BC plans should contain a communications and public information plan to ensure that the readiness level is the maximum possible. Furthermore, the public information plan should set forth policy and procedure to ensure that the agency (and state if appropriate) speaks with one voice in an emergency.

3.2.2 Should Do

- establish and support a “community of practice” for business continuity
- encourage conceptual and culture changes that support business continuity in government
- research, document and coordinate statutory, legal, audit, ethical, policy, fiduciary and regulations provisions related to business continuity

- To facilitate the development of effective continuity in Georgia, a community of practice for business continuity should be established and supported.
    - This community should be manifest in the user group that will come from the GDABC. This group should play a central role in the governance of Georgia’s continuity and recovery planning and action.
    - Members of the community should consult within and across the agencies on areas of best practice in continuity and related matters.
    - The community should provide a vehicle for professional certification in business and government continuity.
    - The community should identify and recommend appropriate best practices and standardization in the area of continuity.

- The community should assist in the credentialing of employees for work in event recovery actions.
- The community should lead the communication, evaluation and assessment of technologies, software and processes for recovery and continuity.
- The community should contribute to the wider body of knowledge about continuity and related areas. Potential contributions include standards, best practices, guidance, policies & procedures, assessments, methods, and models. As appropriate, members of the community should publish and present these contributions to the larger community.

- Effective business continuity will benefit from some organizational "culture changes." These include, but are not limited to:
  - As General Dwight Eisenhower said, "I have always found that plans are useless, but planning is indispensable."
  - For continuity planning to be effective in any organization, leadership must make it a top priority and hold the organization to a constant vigilance and accountability for it.
  - In today's world, any organization's continuity planning and implementation is no longer an option, but mandatory for survival.
  - It is better to have a continuity plan that is approximately right, in place and exercised than one that is detailed but fundamentally flawed or wrong; or worse yet to be paralyzed by over-analysis during planning. For example, if a plan covers most of the possible events in a handful of straightforward factors, it should be preferred over a plan covering 99% of events, but requiring attention to dozens of factors.
  - We must come to understand that planning for contingencies and business continuity is everybody's business, not just the domain of IT.
  - Business continuity is "overwhelming." Planning for continuity is not a one-person job, but instead requires a team to be done effectively. A recovery operation virtually always requires the coordinated effort and cooperation of multiple agencies and often multiple levels of government.

- Research, documentation and coordination of the statutory, legal, audit, ethical, policy, fiduciary and regulatory provisions of continuity as appropriate for Georgia will be of benefit to effective continuity. Such provisions include, but are not limited to:
  - Official procedures and authority for declaring emergencies within the state, county and/or agency should be documented and communicated in a usable form. Similar procedure and authority should be documented and communicated for transitioning through stages including stabilization, recovery operations, and back to normal operations.
  - Policy and procedure should be established and communicated to ensure emergency responses and recovery actions are commensurate with event severity.

- Statutory requirements of emergency action should be documented and communicated.
- Policy and procedure concerning continuity and vital records should be established, documented and/or communicated. Vital records and their role, use and protection in recovery should be covered in continuity plans. Policy and procedure covering the legal and ethical aspects of identity records during emergencies and recovery should receive attention.
- Policy and procedure concerning email and continuity should be addressed.
- Policy and procedure should be established, documented and communicated (along with appropriate supporting technology) for securely storing and distributing operational aspects of the continuity plan to appropriate agency personnel. Procedures and technology for this purpose also must facilitate the timely update of plans and the communication and distribution of those updates.

3.3 Formation of the GDABC Professional Association

A key outcome of the GDABC is the establishment of a users group comprised of participants and other key stakeholders of business continuity/disaster recovery. The major purpose of this group will be to ensure that the effort remains viable in Georgia.

Anticipated actions that the group will undertake during Fiscal Year 2005 follow:

- Assess the current state of business-continuity preparedness by conducting drills in pilot agencies

- Conduct a business-continuity trade show, including vendor demonstrations of software programs that assist with developing business-continuity plans

- Develop a common set of requirements that can be included in all future RFPs related to business continuity

- Develop a plan for business continuity policies and standards that would take effect in FY07

3.4 Requests from Executives

On January 10, 2004, the Chief of Staff for Governor Perdue, Jim Lientz, addressed the GDABC participants at their first user group formation meeting. One of the major outcomes of his presentation was the show of support he voiced for the academy's efforts.

In addition, the participants had formulated a list of suggestions for how the agencies' efforts could be supported in the future. These suggestions will be given to agency and state executives, as appropriate. They include:

- Feedback on our progress
- Support
  - Make continuity preparedness a priority
    - Planning, e.g., request from all agencies
    - Operations, e.g., require exercising of plans
    - Funding, e.g., make continuity a budget priority
  - Expand and maintain Georgia's continuity capability and maturity
  - Attend to and check in about continuity progress

4.0 REFERENCES AND BIBLIOGRAPHY

Following are the major resource documents that were used in the Georgia Digital Academy on Business Continuity.

1. **Business Continuity Planning: A Step-by-Step Guide with Planning Forms**, Kenneth L. Fulmer, Rothstein Associates Inc., www.rothstein.com

2. **Business Continuity Planning: A Step-by-Step Guide with Planning Forms on CD-ROM,** 3rd Edition, Kenneth L. Fulmer, Rothstein Associates Inc., www.rothstein.com

3. **Contingency Planning Guide for Information Technology Systems**, National Institute of Standards and Technology

4. **Disaster Recovery Plan**, Systems Support Inc.

5. **Emergency Management Guide for Business & Industry**, Public-Private Partnership with the Federal Emergency Management Agency

6. **Functional Requirements Phase: Risk and Business Impact Analysis** (a handout), James O. Price, Jr., Certified Business Continuity Planner, Georgia Technology Authority

7. **How to Plan for Workplace Emergencies and Evacuations,** U.S. Department of Labor, Occupational Safety and Health Administration

8. **MIT Business Continuity Plan – 1995**, Massachusetts Institute of Technology

5.0 APPENDICES

APPENDIX A

Senate Bill 243

Senate Bill 243
By: Senators Smith of the 52nd, Mullis of the 53rd, Bowen of the 13th, Tolleson of the 18th, Kemp of the 46th and others

AS PASSED SENATE

A BILL TO BE ENTITLED
AN ACT

To amend Chapter 3 of Title 38 of the Official Code of Georgia Annotated, relating to emergency management, so as to provide that the Georgia Emergency Management Agency shall establish and maintain a standardized, verifiable, performance-based unified incident command system; to provide for the development of and instruction in such command system; to provide for the implementation of such command system; to provide penalties for local agencies that do not establish such command system by December 31, 2004; to provide for related matters; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Chapter 3 of Title 38 of the Official Code of Georgia Annotated, relating to emergency management, is amended by adding a new Code Section 38-3-57 to read as follows:

38-3-57.

(a) The Georgia Emergency Management Agency shall establish and maintain, in collaboration with all appropriate state agencies and volunteer organizations with emergency support function roles, and professional organizations that represent local public safety agencies, including the Emergency Management Association of Georgia, the Georgia Association of Police Chiefs, the Georgia Fire Chiefs´ Association, and the Georgia Sheriffs´ Association, a standardized, verifiable, performance-based unified incident command system.

(b) Such system shall be consistent with the Georgia Emergency Operations Plan and shall be utilized in response to emergencies and disasters referenced in the Georgia Emergency Operations Plan, including Presidentially declared disasters and states of emergency issued by the Governor.

(c) The Georgia Emergency Management Agency, in cooperation with the Georgia Public Safety Training Center, shall develop a course of instruction for use in training and certifying emergency response personnel in unified incident command.

(d) All local public safety and emergency response organizations, including emergency management agencies, law enforcement agencies, fire departments, and emergency medical services, shall implement the standardized unified incident command system provided for in subsection (a) of this Code section by December 21, 2004.

(e) Local agencies that have not established such system by December 31, 2004, shall not be eligible for state reimbursement for any response or recovery related expenseș.

SECTION 2.

All laws and parts of laws in conflict with this Act are repealed.

APPENDIX B

Georgia Digital Academy on Business Continuity

BC Maturity – Core Competency Questionnaire

This questionnaire was developed by James Price of the GTA and is based on the Business Continuity Maturity Model ™ from the Virtual Corporation. Note, BC is used for Business Continuity

Your name: _____ Agency: _____

LEADERSHIP commitment and understanding demonstrated by executive management

- BC is not directed or recognized by the agency's executive management
- The agency management has a (verbal) commitment to BC
- The agency has a formalized governance structure for BC
- That formalized governance includes executive sponsorship
- That sponsoring executive actively participates and is engaged in BC

EMPLOYEE AWARENESS and depth of BC need recognition and activities throughout all staff levels

- BC and Disaster Recovery have limited awareness in the agency
- The agency has limited participation in BC activities
- The agency's BC program has activities to promote BC awareness
- The agency's BC program has activities to promote BC preparedness
- BC and Disaster Recovery are integral parts of the agency's culture

BC PROGRAM STRUCTURE and the scale that it is implemented across the enterprise

- Unstructured, unsystematic, unmeasured and untested
- Understanding/acceptance of the need for BC with some partial solutions
- General awareness and action towards a BC program across the agency
- Integrated and coordinated action towards BC across the agency
- Explicit written structure for BC program integration throughout agency

PERVASIVENESS of BC across the agency

- Only in BC/Disaster Recovery unit
- Limited participation across agency
- Participation by about half the agency
- Integrated and coordinated BC action throughout the agency
- BC planning and action is engrained into the agency's culture

METRICS – Development and monitoring of appropriate measures of BC Program performance

- BC is unmeasured and unmonitored in the agency
- Limited measurement and tracking of BC in the agency
- BC metrics developed and consistently tracked
- Multi-year BC planning and measurements against goals within agency
- Ongoing evaluation with linkage to statewide strategic plan and standards

RESOURCE COMMITMENT for sufficient resources to ensure BC program success

- Few if any resources are committed to BC in the agency
- Limited and spotty coverage of resources for BC in the agency
- The agency has made a commitment to resources for BC
- The agency's resource commitment is tied to strategic plan
- The agency's resource commitment includes BC-qualified staff and assimilates resources throughout the agency

EXTERNAL COORDINATION of BC activities with customers, suppliers and regulators

- BC coordination is externally driven
- Coordination of BC externally is given minimal consideration in the agency
- There is informal external collaboration on BC in the agency
- BC is actively and systematically coordinated with the outside in the agency
- The agency takes a leadership role on external partnerships to benefit BC

APPENDIX C

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day One 9/28/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	

8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP
	• Agenda Review/GDA Overview-Rich H-N
	• In and Out of the Loop-Rich H-N
	• Introductions Round Robin-All (30 Seconds max)
	  • Name
	  • Agency and Role
	  • At the end of the GDABC, I want …
	• Video: "Ready for Anything"- James Price
	• Maturity Questionnaire-James Price
	• SWOT Analysis and BC Goals-Rich H-N	

9:30 AM – 11:00 AM	Breakout Session including 10AM Break-Everyone in facilitated breakout groups • Initial SWOT Analysis • Initial Goals (Fulmer Step 1 pages 6-13) • Maturity Questionnaire with dot vote	
11:00 AM – 11:45 AM	Whole Group Session, Report/Discuss: • Top Significant SWOT • Top Ten Initial Goals/Objectives • Maturity Dot Vote	
11:45 AM – Noon	• Homework: BC Maturity, SWOT and Goals (Fulmer Step 1 and templates #1 - #4) in Your Agency— spend about 90 minutes refining your BC maturity questionnaire responses, SWOT Analysis and doing Fulmer Step 1 for your agency. • Summary of Day 1/Feedback on Day 1/Preview of Day 2/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Two 10/5/04 V2

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Maturity Questionnaire, SWOT Analysis, BC Goals Day 1 Results -Rich H-N • Value Terms & Concepts for BC—Robert Giacomini, OPB • BC Chalk talk—James Price • Dot vote for value and importance on Goals and SWOT	
9:30 AM – 11:00 AM	Breakout Session including 10AM Break-Everyone in facilitated breakout groups --Every group will brainstorm BC Goals (Fulmer Step 1 pages 6-13) • Refine SWOT Analysis (4 groups, one for each) • Refine GDABC Goals (1 group :) • Brainstorm on BC Team Roles (1 group: Fulmer Steps 2 and 3 pages 14-27)	
11:00 AM – 11:45 AM	Whole Group Session, Report/Discuss: • BC Goals • Refined SWOT • Refined Goals/Objectives • BC Team Roles	
11:45 AM – Noon	• Homework: Begin Fulmer Steps 2 and 3 and templates #5 and #6 in Your Agency— spend about 90 minutes for your agency. • Summary of Day 2/Feedback on Day 2/Preview of Day 3/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Three 10/12/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 2 Results -Rich H-N • BC Chalk talk on BC in the GTA—James Price • Robert's Remarks—Robert Woodruff	
9:30AM - 10:00AM	• Dot vote for priorities in briefing slides • Break	
10:00 AM – 11:00 AM	Breakout Session -Everyone in facilitated breakout groups --Every group will discuss staffing the BC Plan (BCP) development (Fulmer Steps 2 and 3 and templates #5 and #6) • Identify job types on your agency's roster (Step 2, Worksheet 5) • Review action items and responsibility assignments (Step 3, Worksheet 6), assessing in your agency: o Number of staff for BCP assignment o Skill level of staff for BCP o BCP resources available in agency o Additional needed BCP resources, training, etc. o Agency BCP dependencies, e.g., GTA, GBA, etc. o Any research required for BCP staffing o Comments on BCP staffing	
11:00 AM – 11:45 AM	Whole Group Session, Report/Discuss: • Briefing priorities • Job Types • Action Items and Responsibility Assignments as reviewed	
11:45 AM – Noon	• Homework: Begin Risk Assessment in Your Agency (Fulmer Step 4, pages 28-48, Worksheet 7) — spend about 90 minutes for your agency. • Summary of Day 3/Feedback on Day 3/Preview of Day 4/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Four 10/19/04 V2

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 3 Results -Rich H-N • Executive Briefing on "Georgia's Business Continuity Preparedness" • GTA Executive Perspective on BC—Cigdem Delano, Deputy Director and Chief Operating Officer, GTA	
9:30AM - 10:00AM	• Proposal—Stan Bush • Voting • Break	
10:00 AM – 11:00 AM	Breakout Session – "Divide and Conquer" and Professionalism & Governance for BC in Georgia	
11:00 AM – 11:45 AM	Whole Group Session, Report/Discuss Breakout Results	
11:45 AM – Noon	• Homework: TBD • Summary of Day 4/Feedback on Day 4/Preview of Day 5/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Five 10/26/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:00AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 4 Results, WebCT -Rich H-N • Review group divisions in light of communities of interest draft	
9:00 AM – 11:00 AM	Breakout Session – "Divide and Conquer" and Professionalism & Governance for BC in Georgia	
11:00 AM – 11:45 AM	Whole Group Session, Report/Discuss Breakout Results	
11:45 AM – Noon	• Homework: TBD • Summary of Day 5/Feedback on Day 5/Preview of Day 6/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Six 11/2/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 5 Results, WebCT -Rich H-N • Risk Assessment and Business Impact Analysis- James Price	
9:00 AM – 11:00 AM	Breakout Session – "Divide and Conquer" and Professionalism & Governance for BC in Georgia	
11:00 AM – 11:45 AM	Whole Group Session, Report/Discuss Breakout Results	
11:45 AM – Noon	• Homework: TBD by Breakout Groups • GTC Check-in • Summary of Day 6/Feedback on Day 6/Preview of Day 7/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Seven 11/9/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:00AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 6 Results, WebCT -Rich H-N • Risk Assessment Process-Wayne Salhany	
9:00 AM – 11:30 AM	Breakout Session –Work on your BC Plans	
11:30 AM – 11:45 AM	Whole Group Session, Report/Discuss Breakout Results	
11:45 AM – Noon	• Homework: TBD by Breakout Groups • GTC Check-in • Summary of Day 7/Feedback on Day 7/Preview of Day 8/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Eight 11/16/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 6 Results, WebCT -Rich H-N • Risk Assessment and Business Impact Analysis – Elaine Townes, DOAS Risk Management	
9:30 AM – 11:30 AM	Breakout Session –Work on your BC Plans	
11:30 AM – 11:45 AM	Whole Group Session, Report/Discuss Breakout Results	
11:45 AM – Noon	• Homework: TBD by Breakout Groups	
Noon to 1PM	Box lunch	
1:00 PM to 3:00 PM	• Facilities Management for Business Continuity—Panel Discussion with Q&A Elliott Penso, Georgia Building Commission, Moderator; Tony Bruehl, DTAE; Mark Demyanek, USG; Frank Smith, GBA	
3:00 to 3:30PM	• Summary of Day 8/Feedback on Day 8/Preview of Day 9/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Nine 11/23/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 8 Results, WebCT -Rich H-N • Sample Business Continuity Plan—James Price	
9:30 AM – 10:50 AM	Breakout Session –Work on your BC Plans (either in breakout groups or independently)	
11:00 AM – 11:55 AM	Whole Group Session: • Pulse Check on Agency BC Plan Status • Small Group Discussions 1 a) T-shirt; b) BC User Group/Certification; c) Develop 2nd Briefing • Small Group Discussions 2 a) GDABC Exercise; b) GDABC Trade Show; c) Develop 2nd Briefing	
11:55 AM – Noon	• Homework: TBD by Agency Needs • Summary of Day 9/Feedback on Day 9/Preview of Day 10/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Ten 11/30/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 9 Results, WebCT -Rich H-N • Andy Taylor and Amelia Winstead – Records and Government Continuity and Georgia Open Records Act	
9:30 AM – 11:30 AM	Breakout Session –Work on your BC Plans (either in breakout groups or independently)	
11:30 AM – 11:55 AM	Whole Group Session: • Pulse Check on Agency BC Plan Status • Presentations on progress	
11:55 AM – Noon	• Homework: TBD by Agency Needs • Summary of Day 10/Feedback on Day 10/Preview of Day 11/Close--All	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Eleven 12/7/04

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register • Find bearings, Settle in Socialize	
8:30AM – 9:30AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 10 Results, WebCT -Rich H-N • Lisa Ray—Public Communications in Emergencies and Government/Business Continuity	
9:30 AM – 11:00 AM	Breakout Session –Work on your BC Plans (either in breakout groups or independently)	
11:00 AM – 11:55 AM	Whole Group Session: • Pulse Check on Agency BC Plan Status • Briefing Review • Survey • Box Lunch	
11:55 AM – Noon	• Homework: TBD by Agency Needs • Summary of Day 11/Feedback on Day 11/Preview of Day 12	
Noon – 12:55PM	• Travel (car pool where possible please) to GEMA State Operations Center—935 E. Confederate Ave. SE; Atlanta, GA 30316; See map	
1:00 - 1:55	• Teresa Harrison, Deputy Regional Administrator of OSHA—Best Practices in Emergency Action Planning and Implementation	
2:00 – 2:30 PM	• Ben Johnson--Tour and Overview of GEMA and the State Operations Center	
2:45 – 3:45 PM	• Cross Government Panel—Q&A Discussion of Cross-Government Communication and Action for Business Continuity	
3:45 – 4:00 PM	• Close	

Georgia Digital Academy Agenda on Business Continuity (GDABC)—Day Twelve 12/14/04—GDABC Graduation!

Time	Activity	Comments
8:00AM -- 8:30AM	• Start-up—Coffee etc. available • Register, Find bearings, Settle in Socialize • BC Maturity Questionnaire and Dot Vote	
8:30AM – 9:15AM	• Logistics/Meeting Guidelines/VMDP • Review: Agenda, Day 11 Results, WebCT -Rich H-N • BC Maturity Questionnaire and Dot Vote—Finalize • Georgia's Continuity Maturity—James Price • Review of Proposed GDABC Recommendations and Next Steps	
9:15 AM – 9:45 AM	Break with • Pulse Check on Agency BC Plan Status • Dot vote on GDABC Recommendations • Dot vote on Topic for Next GDA • "Garage-sale" Valuation of Next Steps	

9:45 AM – 10:55 AM	• Final GDABC Rating Survey
	• Whole Group Session to Review ("Meat & Potatoes" of GDABC Briefing and Report):
	  • Pulse Check
	  • GDABC Recommendations
	  • Topic for Next GDA
	  • Valuation of Our Next Steps	

10:55 AM – 11:30 AM	• Adjourn GDABC • Group Picture in 1514ABC • Move to Stately Events Room, 20th Floor West Tower	
11:30 AM – 1:45 PM	• GDABC Graduation in Stately Events Room, 20th Floor West Tower	

APPENDIX D

SPSU Research into a Sample of Current State Activities

GEORGIA DIGITAL ACADEMY

MERCY GITURO
DR. RICH HALSTEAD-NUSSLOCSH

STATE BUSINESS CONTINUITY PLANS

FLORIDA

People, Planning Key to Business Continuity by Michael Pastore

He explains "it doesn't take 9-11 to bring a business to its knees. Information that is the lifeblood of your organization should be at the top"

http://www.cioupdate.com/trends/article.php/2244581

Storms unlikely to cloud Florida's business future by Robert Trigaux

Business confidence in Florida's weather
http://www.sptimes.com/2004/10/03/Columns/Storms_unlikely_to_cl.shtml

Blueprint for Survival by Christine Winter

Business plot strategies for dealing with catastrophe's -
Planning for the worst has always been part of doing business in South Florida. But since 9-11, it has become a matter of corporate responsibility for companies large and small, public and private, to set up detailed plans on how to save and access their data, protect and round up their employees and keep the business running after a disaster, whether at the hands of Mother Nature or terrorists.

http://www.agilityrecovery.com/news/articles/june2003/sentinel.htm

Southeast Florida Association of Contingency Planners is the Premier Organization of contingency planners, business continuity professionals and emergency managers on the east coast of South Florida. Southeast Florida Association of Contingency Planners provides members an excellent information exchange experience and opportunities to set emergency response and recovery trends

http://www.acp-international.com/seflorida/index.htm

State, local officials support Business Continuity Planning by Steve Letzler

The Depository Trust & Clearing Corporation (DTCC) announced in May that it would open a new operations facility in Tampa that will also help ensure the company's ability to continue to operate in the event of a major regional emergency.

http://www.dtcc.com/Publications/dtcc/jun04/tampa.html

http://securitysolutions.com/mag/security_frances_charley_teach/

Tools

This self-assessment is an optional tool for local authorities. It aims to provide a framework against which authorities can review current performance and identify areas for improvement

http://www.audit-commission.gov.uk/emergencyplanning/index.asp

http://www.softscout.com/A556CC/softscout.nsf/F_BROWSE?OpenForm&Category=Operations.Continuity%20Planning

GEORGIA

Living with Terror by Malcolm Wheatley

Nearly six years before Sept. 11, 2001, Citibank, the Pittsford, N.Y.-based multinational financial services company, became starkly aware how vulnerable its operations were to terrorist attacks.

http://www.cio.com/archive/021502/terror.html

International and Homeland Security by Calvin Sims

Americans are closely divided on whether they think the United States is prepared to deal with another terrorist attack, but the overwhelming majority has done nothing to prepare for such an attack themselves, according to a recent New York Times poll.
The poll found that most Americans are not worried that they or a family member will become a victim of terrorism, with the majority of the respondents saying they do nothing different even when the government raises the terror-alert level.

http://homelandsecurity.osu.edu/focusareas/citizen.html

Terrorism – The Ultimate Wild Card – by Jennifer Caplan, CFO.com

Eight months after the worst terrorist attack in U.S. history, finance chiefs say they are still concerned about the prospect of another assault on American soil. This pervasive fear was underscored by a recent survey of 200 chief financial officers, treasurers, and risk managers. In the survey (conducted by FM Global, the National Association of Corporate Treasurers, and Sherbrooke Partners), more than half of the respondents said their companies are not well prepared for an interruption to their businesses.

What's more, forty-three percent of the surveyed finance executives said a major disruption to their businesses' top earnings driver would either cause sustained damage to their companies' income or

severely threaten business continuity. Only 24 percent thought such a loss would be a one-time hit to earnings.

http://www.cfo.com/printable/article.cfm/3004648?f=options

Information Technology Security and Business Continuity

Recognizing a need for increased computer security; companies have shifted significant portions of their information technology (IT) budgets to fund security solutions. However, most companies focus heavily on the technical components of security, all too often ignoring the need for an overall security strategy. This program provides the rationale for an overall security strategy and presents guidelines for assessing policy gaps, developing new policies, and doing periodic re-evaluation. The session also provides a framework for developing a comprehensive business continuity plan that goes beyond IT security and encompasses the critical business processes of the firm.
http://www.pe.gatech.edu/conted/servlet/edu.gatech.conted.course.ViewCourseDetails?COURSE_ID=468

Southeast Continuity Planners Association (SCPA)

This Business Continuity, Disaster Recovery, and Emergency Management information exchange group is open to all interested public and private sector individuals seeking to discuss common issues surrounding the contingency planning industry. We are an independent and non-fee-based organization, which seeks to promote cross-sector discussions revolving around the continuity of both business and community in the event of an unplanned interruption of life, as we know it. Although Atlanta GA-based, we have members from each border state and across Georgia and encourage interested parties from throughout the Southeast to join the group and participate in our quarterly meetings and ad-hoc seminars.

http://www.drj.com/groups/scpa.htm

NORTH CAROLINA

Business Continuity Best Practices in North Carolina by Katherine White.

Any number of threats can strike a state and its government agencies. In the last three years alone, North Carolina has been hit with Hurricane Floyd, tornadoes and extraordinary snow and ice storms. The state's information technology systems have been threatened with denial of service attacks and insidious worms.

A single event – whether manmade or natural – can jeopardize the state's information technology resources, which in turn, can hinder the delivery of critical services to the state's citizens and government agencies. The North Carolina Office of Information Technology Services (ITS) is the principal provider of networking, telephone, distributed systems, and mainframe services for state government. Recognizing the need for continuity of the IT infrastructure services that it provides to government, ITS established a business continuity program that develops realistic plans for recovery of IT systems in case of a disaster.

http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-NorthCarolina_R2GVI8_0Z5RDZ-i34K-pR.htm

Business Continuity Management by ITS

Policy

ITS, under the direction of the ITS Security Office, shall support business continuity and disaster recovery by maintaining and periodically testing comprehensive business continuity plans in order to resume business as quickly as possible following an outage, regardless of the probable cause.

Business recovery activities can take on different forms of resumption depending on the nature of the outage. Short-term outages such as power failures, system internal failures, etc., are minimized by the

redundancy of computer system components. Long-term outages (greater than two days) can recover at an alternate computing site to provide critical services to the citizens of North Carolina.

http://www.its.state.nc.us/Support/Security/SecurityRecovery.asp

North Carolina's Technology Project Named Best in the Nation by Michael F. Easley – Governor

Raleigh - The National Association of State Chief Information Officers (NASCIO) selected North Carolina's Business Continuity Management Improvement Project as the best in the nation in the area of business and continuity planning. The program established by the Office of Information Technology Services (ITS) under State Chief Information Officer George Bakolia and Chief Security Officer Ann Garrett, provides business continuity services for the state's mainframe and telecommunications infrastructure.

http://www.nc.gov/asp/subpages/news_release_view.asp?nrid=404

North Carolina Business Continuity and Recovery Services
2002 NASCIO Award Winner

Recognizing the need for continuous service in response to any number of threats and natural disasters, the North Carolina Office of Information Technology Services (ITS) established a business continuity program. The program has three full-time employees who work with ITS and its customers to develop realistic plans for recovery of the systems in case a catastrophe destroys either accessibility to the application or the application itself.

http://www.nga.org/center/egovernment/confidencelep/1,1461,,00.html

Tools

Business Continuity Planning by Fidelity Capital Management

Business Continuity Planning

Just the Facts ...

- What happens to my business in the event of my death, disability, or retirement?
- How will my family or I get money out of the business on a tax-favored basis?
- Who will ultimately run my business? Will my children want to be involved?
- If I sell the business, how should the sale be structured?

To help answer your questions, Fidelity Capital Management reviews in detail your existing business continuity plan, identifying all aspects of the current planning strategy that may improve or threaten the succession of your business.

http://fidelitycapitalmanagement.com/cont.htm

Mission:

Formed to share information about Contingency Planning. These disciplines involve the planning, and preparation for resumption of business in the event of a disaster.

Objectives:

Provide a forum for the interchange of ideas, topics, and information in the field of business contingency planning.

Promote increased awareness of business contingency planning.

Identify common problems and propose resolutions.

Identify supplier requirements, which could facilitate business contingency planning.

Encourage public and private partnerships to ensure collaboration across the community.

http://www.drj.com/groups/bcpc/

MISSOURI

Business Continuity for the State of Missouri

The State of Missouri has a robust and diverse information technology infrastructure that contains some leading edge technology, which has been applied to business processes in some very innovative ways. The infrastructure is diverse in that segments of it can be found in every agency in the State. The State's ability to effectively conduct business has come to rely upon the continuous availability of that information technology infrastructure.

Business Continuity Management (BCM) relates specifically and significantly to state agencies' ability to continue to conduct business in catastrophic conditions or severe infrastructure failures to ensure the maximum availability of essential services. Business Continuity Management is a business issue, with real benefits for any organization and must be considered an organization wide discipline with support from top management.

http://oit.mo.gov/initiatives/business%20continuity.html

Dept. of Revenue – plans to recover business operations after a disaster – by Claire McCaskill

This audit analyzed the Department of Revenue's capability to resume normal business operations and recover information from automated data systems after a disaster or other disruptive event. Auditors examined disaster recovery planning, staff emergency response training, as well as testing and documentation procedures for backup systems and environmental controls. In the last year, department officials began to develop and implement a continuity plan. Audit results identified areas to enhance this plan.

http://www.auditor.state.mo.us/press/2002-85.htm

MICHIGAN

Michigan awarded again for Excellence in Information Technology

Michigan's second award came in the "Security and Business Continuity" category, with the selection of the Michigan Critical Incident Management System. To address an outdated information management

system at the State Emergency Operations Center (SEOC), the E Team Critical Incident Management System (CIMS) software application was selected as the preferred information management tool. E Team was installed on computers in the SEOC in conjunction with the GIS mapping software, and because E Team is a web based application, it is now being used by all state agencies, over 110 local emergency management programs, numerous local police, fire, emergency medical technicians, hospital/medical facilities, other emergency responders, and critical infrastructures within Michigan.

http://www.michigan.gov/msp/0,1607,7-123-1586_1710-103180--,00.html

Security and Business Continuity

During the power blackout that affected a large portion of the northeast United States in August 2003, the CIMS proved invaluable and was used extensively by state agencies within the SEOC. The Michigan Department of Information Technology (MDIT) used the CIMS to display information generated by the SEOC and other state agencies in its agency's Emergency Coordination Center during the blackout emergency proving the system's value for internal communications.

http://www.nascio.org/awards/2004awards/security.cfm

Continuity e-Guide by Disaster Resource Guide

Business Continuity: Now What?

The Sarbanes-Oxley Act (SOA) mandates reporting of and controls over many types of risks facing an enterprise's financial reporting process. However, in a surprise release last week, an accounting oversight board recommended SOA Section 404, apart from rather specific data backup requirements, makes no requirements for corporate-wide business continuity planning. Does the recommendation even make sense? Or equally important, does this impact executive management's support for business continuity?

http://www.disaster-resource.com/newsletter/continuityv24.htm

MSU study finds supply chain often neglected in business continuity planning by Jeff Ashcroft

EAST LANSING, Mich. – A Michigan State University study commissioned by AT&T has found that companies are courting disaster if their business plans fail to ensure supply-chain continuity.

The findings suggest that supply chains have become increasingly fragile. When something does go wrong, the event and the resulting supply-chain disruption can have a significant – if not catastrophic – impact on the buying firm.

Consequently, managers working within "best practice" companies have developed an awareness of these potential risks and, more importantly, they have introduced systems and procedures aimed at proactively managing the risk. The result is not only better performance, but also the emergence of a potentially important competitive advantage.

http://mba.bus.msu.edu/news/index.cfm?newsid=409

http://logistics.about.com/b/a/087849.htm

http://www.emc.com/solutions/continuity/index.jsp

KENTUCKY

Kentucky Revamps, Reforms, and Scores – by Tracy Heath

The continuity that is most impressive in northern Kentucky is that of its business location successes.

http://www.siteselection.com/features/2000/mar/ky/pg02.htm

Provide quality, business continuity and recovery education networking and support to risk, continuity, and emergency professionals in the Kentucky, Southern Indiana and Ohio areas. Our goal is to provide access to local, regional and national contingency and emergency response professionals and organizations for development and educational opportunities.

This professional group consists of continuity and emergency response planners and managers from the public and private sector. We want our program to cover various topics of interest to continuity and emergency planners inspired by our changing world and the demands of our profession. CEU credits are available for most professionals. Some topics under discussion are:

- Business Impact Analysis
- Emergency Response
- Exercise and Testing
- Physical Security and Safety
- Risk Assessment
- Plan Development
- Team building
- Project management for business continuity managers
- Maintenance lifecycle
- Working with local, regional, and national agencies during cries
- Business Continuity Certification

To make this effort successful and provide the best in Business Continuity support, networking, and education, we need you.
http://www.drj.com/groups/kcp.html

VIRGINIA

Business Continuity Planning

The purpose of business continuity planning is to provide for the continuation of critical business functions in the event of disruptions. Preparation for handling disaster contingencies is generally called business continuity planning or contingency management. A secondary purpose of business continuity planning is to minimize the effect of disruptions. Many potential contingencies and disasters can be averted, or the damage they cause reduced, if appropriate steps are taken early to control the event.

http://www.vascan.org/checklist/business_continuity_check.html

Physical Infrastructure - Homeland Defense Training Conference

About This Conference - The nation's physical infrastructure enables the flow of the vital goods and services that keep our government and our society operating smoothly. Comprised of roads, railroads, pipelines, power plants, dams, power lines, water treatment plants and many more types of assets; the physical infrastructure supports numerous critical government functions. Protecting such a broad spectrum of infrastructure requires a broad range of approaches; from traditional facility security for dams or water treatment plants to more network-centric methods of characterizing vulnerabilities of electric power grids or pipeline networks.

In the post-September 11th environment, it is necessary for government managers to be able to identify key dependencies on physical infrastructure and assess the impacts of the potential loss of infrastructure.

http://www.homelanddefensejournal.com/conf_phys_sec2.htm

Business Recovery Association of Virginia

The **B**usiness **R**ecovery **A**ssociation of **V**irginia is an independent professional association of those involved in Business Continuity/Recovery and Contingency Planning. Membership is open to anyone who would like to participate. There are no membership dues or meeting fees. Leadership is by an informal Steering Group. Meetings are held quarterly at host sites, generally in the Richmond area.

http://www.drj.com/groups/brav/brav.htm

INDIANA

Making the case for Business Continuity – by Geary Sikich

Traditionally, business continuity professionals have had a limited role in corporate management activities. This role has been mainly to address aspects of 'crisis' response, mainly regulatory driven or in reaction to a crisis situation. However, when we start to rethink the role that business continuity professionals can play in today's global environment we see that the role is more than developing 'bookshelf plans.' The business continuity professional's role should focus on a comprehensive structuring of initiatives designed to establish and maintain resilience between and among all the touch points of the enterprise.

http://www.continuitycentral.com/feature0144.htm

Midwest Contingency Planners

Midwest Contingency Planners is a not for profit organization. We serve as a forum for business professionals working in the areas of business continuity, business resumption, contingency planning, disaster recovery and other related emergency recovery functions. Our membership area covers Indiana and surrounding states.

http://www.drj.com/groups/mcp/MCPindex.htm

http://www.drj.com/groups/mcp/aboutMCP.htm

OHIO

Homeland Security Focus Areas – Citizen & Volunteer Activities by Calvin Sims

While domestic security has been a major issue in the presidential campaign with Republicans and Democrats warning that another terrorist attack is inevitable, the Times poll suggests that for most Americans the issue is not a preoccupation.

In the survey, 46 percent of the respondents said they did not think the United States was prepared for a terrorist attack, while 43 percent said the country was prepared.

http://homelandsecurity.osu.edu/focusareas/citizen.html

Contingency **Planners of Ohio – Are you ready for the unexpected?**

Welcome to the Contingency Planners of Ohio's Web Site. We are a long-established association of professionals dedicated to sharing expertise, education, and experiences to improve the preparedness, response, mitigation, and recovery of businesses from disasters and emergencies, which affect their corporation, customers, and communities.

http://www.cpohio.org/

KANSAS

Preparedness through Partnership

The Partnership for Emergency Planning, PEP, is a partnership of private businesses and public sector service agencies. It is a public/private partnership of individuals who come together to share and become better prepared to respond to an emergency and recover from a disaster.

PEP was founded in 1989 as a non-profit organization dedicated to emergency planning issues in the metropolitan Kansas City area. Membership has expanded over the past years and now includes

hospitals, school districts, municipalities, federal, state and local emergency management associations, and some of the largest corporations in Missouri & Kansas. Membership representation now reaches out from the core of Kansas City to other outlying regions.

PEP maintains a goal to facilitate the exchange of information between the private and public sectors and promote community-wide awareness of the importance of emergency planning and disaster recovery.

PEP's primary focus areas are:

- The protection of employees and assets
- Maintaining business continuity through mitigation, crisis management and recovery following a disaster.

PEP Objective

PEP facilitates resources for members:

- To network in their respective emergency/disaster planning process;
- To present information concerning public services agencies and recovery interactions; and
- To share resources and lend assistance between agencies and companies.

http://www.pepkc.org/

TENNESSEE

Business Continuity / Disaster Recovery Manager by Thomas B. Gordon, Jr.

Project and Program Management Professional with over 14 years of extensive experience in telecommunications, data, networks, computer, information systems and technology management. Directly responsible for process design and development, project management, program management and team leadership in multiple business environments.

http://www.newfocus.net/iaem/forum/DCForumID3/311.html

Assuring Business Availability -in the Spotlight

Business challenge

For over 50 years, BlueCross BlueShield of Tennessee has built a solid reputation on providing reliable and affordable health care services to local Tennesseans who depend on the Plan (independent, locally operated companies of BlueCross BlueShield are called Plans).

To maintain reliability and quality, the enterprise system personnel department has become a continuous data processing center, relying on varied computing environments to process approximately 80,000 medical claims a day. The key to processing those medical claims involves having a backup and recovery utility in place to protect and restore valuable data and continue business processes.

"Without a backup and recovery tool in place, we risk losing either online data from over 2,800 users or potential dollars from the loss of productivity. For us, business continuity is a priority and serves as a critical aspect in meeting the needs and expectations of some 4,300 employees and 2.9 million people," says AIX system administrator Dean Holland.

As a not-for-profit company, BlueCross BlueShield of Tennessee holds a competitive 35% market share in the state's health care industry; and keeping that competitive edge means using tools that yield advantages.

http://www.bmc.com/about/spotlight/bluecross_blueshield_of_tennessee_1002_lite.html

NEW HAMPSHIRE

Governor Heeds Call of Manufacturing Community;

Adds Category to $250,000 Business Plan Competition

By Kevin Smith

MANCHESTER, NH - Saying that the "ongoing health of the state's manufacturing industries is a top priority," Governor Craig Benson announced that manufacturing now merits a category of its own in the 2005 Start Up New Hampshire $250,000 business plan competition which celebrated its kickoff at the Palace Theatre this afternoon.

"One month ago at the state Manufacturing Summit, I learned about all of the great ideas that are circulating in New Hampshire's manufacturing community and knew that this competition could help stimulate even more activity," Governor Benson said. "Keeping manufacturing growing and thriving is vitally important and moving great ideas into implementation is what Start Up New Hampshire is all about."

Start Up New Hampshire is an innovative public/private partnership designed to encourage the creation of new businesses in the Granite State. The competition, funded by Public Service of New Hampshire, offers cash prizes totaling $250,000, making the initiative the largest business plan competition in the United States.

http://www.nh.gov/governor/pr_10_26_04businessplan.html

ALABAMA

Homeland Security – Press Releases

Throughout the month of September, hundreds of activities are planned to highlight the importance of individual emergency preparedness. The National Preparedness Month coalition, which includes the U.S. Department of Homeland Security, more than 80 organizations and all 56 states and territories, will encourage Americans to take simple steps now to prepare themselves and their families for any possible emergencies.

http://www.dhs.gov/dhspublic/display?content=3963

Avoiding Disaster: how to keep your business going when catastrophe strikes –

by John Laye FBCI

When disaster strikes, it offers business leaders the peace of mind of knowing that their business is ready for any contingency, no matter how extreme. This guide is designed to be use as both a preparatory resource for when times are good, and an emergency reference when times are bad. This book gets managers up-to-speed on what they should be prepared to deal with and offers real solutions for putting those business continuity plans in place. From natural and man-made disasters to catastrophic computer hack attacks, when disaster strikes is the ultimate weapon for any manager determined to help the business survive no matter what.

"Avoiding Disaster is comprehensive, accurate, and exceptionally useful. It is written for the corporate manager/executive tasked with developing and/or managing the strategic function the author calls 'disaster avoidance.' This book provides the best description I have seen of what should be done, and what skills and knowledge are required to do it. I designed and teach the graduate-level course in Corporate Crisis Management and Business Continuity in the George Washington University's Crisis, Emergency, and Risk Management degree program. I intend to use John Laye's book as a text."

http://www.businesscontinuity.com/page0.htm

South East Business Recovery Exchange

by Scott Hall, CBCP – President

John Fason – Vice President of Planning
Maggi Johnsen, CRM – Vice President of Membership

The South East Business Recovery Exchange is an informal organization that promotes the interaction of persons involved in, or responsible for, disaster recovery/business continuity planning in their respective organizations. The mission of the group is to effectively serve the membership through professional excellence by providing a forum for information exchange. Membership eligibility will be to employees of companies, which have a disaster recovery/business continuity function or otherwise have an interest in establishing such a function. Businesses whose source of revenue is derived from the sale of disaster recovery/business continuity products and services are not eligible for membership.

http://www.drj.com/groups/sebre.htm

Tools
Business Continuity Planning Software

Business Continuity Planning System Version 3.0
The potential loss to your organization that a system disruption could cause is staggering. Because so may aspects of your business hinge on your systems' reliability, your Business Continuity Plan (BCP) will be quite extensive and may be difficult to organize and maintain. We offer BCP software and training to help you manage and ensure the effectiveness of your Plan.

http://www.rsmmcgladrey.com/Services/Detail/bcp_software.html
Business Continuity Awards –
2002 NASCIO Recognition Awards

Security & Business Continuity

Winner: North Carolina – this report is detailed below with a link providing the complete report.
Second place: Washington
Transact Washington
Third place: Virginia
Virginia Security Awareness Training (VASAT) enterprise service

DRJ Contingency Group Contacts by state and by associations
http://www.drj.com/groups/drj6.html

Business Continuity Winner Report – North Carolina
North Carolina Digital Government Application – Security and Business Continuity 2002
The North Carolina Office of Information Technology Services (ITS) is the nerve center for state technology. It is the principal provider of telephony, distributed systems, and mainframe services for state government. Because government relies heavily on information technology for its critical operations, the availability of information technology must be assured.

Recognizing the need for continuous service, ITS established a business continuity program. The program has three full-time employees who work with ITS and its customers to develop realistic plans for recovery of the systems in case a catastrophe destroys either accessibility to the application or the application itself.

The ITS Business Continuity Plan (BCP) has as its highest priority the protection of people. The second focus is data backup, with all records being copied and stored at a remote off-site facility. The third element is the provision of alternate locations, complete with compatible computers and telephones, and up-to-date contact numbers for employees, contractors and customers.

Emergency systems are tested. Several times a year ITS conducts "hot site" drills at emergency locations where information technology systems are recovered on a remote basis. The tests ensure that critical applications, ranging from criminal history records to food distribution tracking to radioactive waste repositories, can be brought on line within 24 hours.

The plan is inherently flexible, able to respond to diverse situations. For example, a software failure earlier this year activated two plans simultaneously: 1) ITS called the software vendor to the site; and, 2) ITS loaded critical tapes onto trucks for transport to a hot site in Philadelphia. Had the vendor not been able to fix the problem, the hot site would have been prepared to operate systems remotely. The ITS business recovery services contractor also provides mobile data centers based in 18-wheel trucks, should such a backup be necessary.
http://www.nascio.org/awards/2002awards/security.cfm

Appendix E

Final GDABC Evaluation Form

Georgia Digital Academy on Business Continuity--Overall Evaluation—12/14/04

Directions: Please rate your level of satisfaction with the overall GDABC in each of the areas below. Provide comments and suggestions for improvement, especially for those areas that were not satisfactory for you. Please use the opposite side if necessary. Leave blank any item that is not applicable to you. Thanks.

GDABC Area	Very Satisfied	Satisfied	Neither	Dissatisfied	Very Dissatisfied
Your overall **Educational Experience**, that is the GDABC as an environment for you to learn more about Business Continuity, IT across the state, the GTA, other agencies, your colleagues, etc. Comments:	❑	❑	❑	❑	❑
Your overall **Teamwork Experience**, that is the GDABC as an environment for teamwork towards solving common problems in your agency and across the statewide enterprise and in other agencies, etc. Comments:	❑	❑	❑	❑	❑
Your overall **Technical Experience**, that is the GDABC as an environment for you to hear of and acquire the best technical practices for business continuity planning & implementation for your agency and across the state, etc. Comments:	❑	❑	❑	❑	❑
Your overall **Business Experience**, that is the GDABC as an environment for you to hear of and acquire best business practices for business continuity planning & implementation for your agency and across the state, etc. Comments:	❑	❑	❑	❑	❑
The GDABC support for **Logistics, Registration, Communications, Refreshments, etc.** Comments:	❑	❑	❑	❑	❑
The GDABC support for **Getting Buy-in & Communicating about Business Continuity within Your Agency.** Comments:	❑	❑	❑	❑	❑

The GDABC support for **Starting or Improving the Business Continuity Plan within Your Agency.** Comments:	❑	❑	❑	❑	❑
The GDABC support for **Sustaining Business Continuity Action within Your Agency.** Comments:	❑	❑	❑	❑	❑
The GDABC support for **Business Continuity Planning and Action Statewide** Comments:	❑	❑	❑	❑	❑

What was the most valuable experience for you or your agency in the GDABC? Why?

What was the least valuable experience for you or your agency in the GDABC? Why?

What might we do to improve the GDABC or the overall GDA process? Please provide details.

Would you recommend the GDA to another State professional? Why or why not?

Do you have any additional comments or recommendations about the GDA or GDABC not covered above?

Appendix F

Glossary of Terms

The definitions in this glossary were developed by the Disaster Recovery Journal, (www.drj.com), in conjunction with Disaster International, DRI, 2003. Used with the permission of DRJ.

1. **ACTIVATION**: The implementation of business continuity capabilities, procedures, activities and plans in response to an emergency or disaster declaration; the execution of the recovery plan.
2. **ALERT**: Notification that a potential disaster situation exists or has occurred; direction for recipient to stand by for possible activation of disaster recovery plan.
3. **ALTERNATE SITE**: An alternate operating location to be used by business functions when the primary facilities are inaccessible. (1) Another location, computer center or work area designated for recovery. (2) Location, other than the main facility, that can be used to conduct business functions. (3) A location, other than the normal facility, used to process data and/or conduct critical business
   functions in the event of a disaster. *SIMILAR TERMS*: Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility, Backup Location, Recovery Site.
4. **ALTERNATE WORK AREA**: Office recovery environment complete with necessary office
5. infrastructure (desk, telephone, workstation, and associated hardware, communications, etc.); also referred to as Work Space or Alternative work site.
6. **APPLICATION RECOVERY**: The component of Disaster Recovery that deals specifically with the restoration of business system software and data, after the processing platform has been restored or replaced. SIMILAR TERMS: Business System Recovery.
7. **BACKUP GENERATOR**: An independent source of power, usually fueled by diesel or natural gas.
8. **BUSINESS CONTINUITY INSTITUTE** (BCI, www.thebci.org): A not-for-profit organization that offers certification and educational offerings for business continuity professionals.
9. **BUSINESS CONTINUITY PLANNING** (BCP): Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change. *SIMILAR TERMS*: Contingency Planning, Disaster Recovery Planning.
10. **BUSINESS CONTINUITY PROGRAM**: An ongoing program supported and funded by executive staff to ensure business continuity requirements are assessed, resources are allocated and, recovery and continuity strategies and procedures are completed and tested.

11. **BUSINESS CONTINUITY STEERING COMMITTEE**: A committee of decision-makers, business owners, technology experts and continuity professionals, tasked with making strategic recovery and continuity planning decisions for the organization.
12. **BUSINESS IMPACT ANALYSIS** (BIA): The process of analyzing all business functions and the effect that a specific disaster may have upon them. 1) Determining the type or scope of difficulty caused to an organization should a potential event identified by the risk analysis actually occur. The BIA should quantify, where possible, the loss impact from both a business interruption (number of days) and a financial standpoint. SIMILAR TERMS: Business Exposure Assessment, Risk Analysis
13. **BUSINESS INTERRUPTION**: Any event, whether anticipated (e.g., public service strike) or unanticipated (e.g., blackout) which disrupts the normal course of business operations at an organization location.
14. **BUSINESS INTERRUPTION COSTS**: The costs or lost revenue associated with an interruption in normal business operations.
15. **BUSINESS INTERRUPTION INSURANCE**: Insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster.
16. **BUSINESS RECOVERY COORDINATOR**: An individual or group designated to coordinate or control designated recovery processes or testing. *SIMILAR TERMS*: Disaster Recovery Coordinator
17. **BUSINESS RECOVERY TIMELINE**: The chronological sequence of recovery activities, or critical path that must be followed to resume an acceptable level of operations following a business interruption. This timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.
18. **BUSINESS RESUMPTION PLANNING** (BRP): TERM Currently Being Reworked. SIMILAR TERMS: Business Continuity Planning, Disaster Recovery Planning
19. **BUSINESS RECOVERY TEAM**: A group of individuals responsible for maintaining the business recovery procedures and coordinating the recovery of business functions and processes. SIMILAR TERMS: Disaster Recovery Team
20. **BUSINESS UNIT RECOVERY**: The component of Disaster Recovery which deals specifically with the relocation of a key function or department in the event of a disaster, including personnel, essential records, equipment supplies, work space, communication facilities, work station computer processing capability, fax, copy machines, mail services, etc. *SIMILAR TERMS*: Work Group Recovery.
21. **CALL TREE**: A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.
22. **CERTIFIED BUSINESS CONTINUITY PROFESSIONAL** (CBCP): The Disaster Recovery Institute International (DRI International), a not-for-profit corporation, certifies CBCPs and promotes credibility and professionalism in the business continuity industry. Also offers MBCP (Master Business Continuity Professional) and ABCP (Associate Business Continuity Professional).
23. **CHECKLIST EXERCISE**: A method used to exercise a completed disaster recovery plan. This type of exercise is used to determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.
24. **COLD SITE**: An alternate facility that already has in place the environmental infrastructure required to recover critical business functions or information systems, but

does not have any pre-installed computer hardware, telecommunications equipment, communication lines, etc. These must be provisioned at time of disaster. *SIMILAR TERMS*: Shell Site; Backup Site; Recovery Site; Alternate Site.

25. **COMMUNICATIONS RECOVERY**: The component of Disaster Recovery, which deals with the restoration, or rerouting of an organization's telecommunication network, or its components, in the event of loss. *SIMILAR TERMS*: Telecommunications Recovery, Data Communications Recovery
26. **COMPUTER RECOVERY TEAM**: A group of individuals responsible for assessing damage to the original system, processing data in the interim, and setting up the new system.
27. **CONSORTIUM AGREEMENT**: An agreement made by a group of organizations to share processing facilities and/or office facilities, if one member of the group suffers a disaster. SIMILAR TERMS: Reciprocal Agreement.
28. **COMMAND CENTER**: Facility separate from the main facility and equipped with adequate communications equipment from which initial recovery efforts are manned and media-business communications is maintained. The management team uses this facility temporarily to begin coordinating the recovery process and its use continues until the alternate sites are functional.
29. **CONTACT LIST**: A list of team members and/or key players to be contacted including their backups. The list will include the necessary contact information (i.e., home phone, pager, cell, etc.) and in most cases be considered confidential.
30. **CONTINGENCY PLANNING**: Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.
31. **CONTINGENCY PLAN**: A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations. A contingency plan may use any number of resources including workaround procedures, an alternate work area, a reciprocal agreement or replacement resources.
32. **CONTINUITY OF OPERATIONS PLAN** (COOP): A COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. This term traditionally is used by the Federal Government and its supporting agencies to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption or Contingency Planning.
33. **CRATE & SHIP**: A strategy for providing alternate processing capability in a disaster, via contractual arrangements with an equipment supplier, to ship replacement hardware within a specified time period. *SIMILAR TERMS*: Guaranteed Replacement, Drop-Ship, Quick Ship.
34. **CRISIS**: A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation or ability to operate.
35. **CRISIS MANAGEMENT**: The overall coordination of an organization’s response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.
36. **CRISIS MANAGEMENT TEAM**: A crisis management team will consist of key executives as well as key role players (i.e. media representative, legal counsel, facilities

manager, disaster recovery coordinator, etc.) and the appropriate business owners of critical organization functions

37. **CRISIS SIMULATION**: The process of testing an organization's ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.
38. **CRITICAL FUNCTIONS**: Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.
39. **CRITICAL INFRASTRUCTURE**: Systems whose incapacity or destruction would have a debilitating impact on the economic security of an organization, community, nation, etc
40. **CRITICAL RECORDS**: Records or documents that, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or recreation at considerable expense.
41. **DAMAGE ASSESSMENT**: The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc., and determining what can be salvaged or restored and what must be replaced.
42. **DATA BACKUPS**: The back up of system, application, program and/or production files to media that can be stored both on and/or offsite. Data backups can be used to restore corrupted or lost data or to recover entire systems and databases in the event of a disaster. Data backups should be considered confidential and should be kept secure from physical damage and theft.
43. **DATA BACKUP STRATEGIES**: Those actions and backup processes determined by an organization to be necessary to meet its data recovery and restoration objectives. Data backup strategies will determine the timeframes, technologies, media and offsite storage of the backups, and will ensure that recovery point and time objectives can be met.
44. **DATA CENTER RECOVERY**: The component of Disaster Recovery that deals with the restoration, at an alternate location, of data centers services and computer processing capabilities. SIMILAR TERMS: Mainframe Recovery, Technology Recovery.
45. **DATA RECOVERY**: The restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last safe backup.
46. **DATABASE REPLICATION**: The partial or full duplication of data from a source database to one or more destination databases. Replication may use any of a number of methodologies including mirroring or shadowing, and may be performed synchronous, asynchronous, or point-in-time depending on the technologies used, recovery point requirements, distance and connectivity to the
47. source database, etc. Replication can if performed remotely, function as a backup for disasters and other major outages. *SIMILAR TERMS*: File Shadowing, Disk Mirroring.
48. **DISK MIRRORING**: Disk mirroring is the duplication of data on separate disks in real time to ensure its continuous availability, currency and accuracy. Disk mirroring can function as a disaster recovery solution by performing the mirroring remotely. True mirroring will enable a zero recovery point objective. Depending on the technologies used, mirroring can be performed synchronously, asynchronously, semi-synchronously, or point-in-time. *SIMILAR TERMS*: File Shadowing, Data Replication, Journaling.

49. **DECLARATION**: A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged mitigating actions (e.g., a move to an alternate site).
50. **DECLARATION FEE**: A one-time fee, charged by an Alternate Facility provider, to a customer who declares a disaster. NOTE: Some recovery vendors apply the declaration fee against the first few days of recovery. 1) An initial fee or charge for implementing the terms of a recovery agreement or contract. SIMILAR TERMS: Notification Fee.
51. **DESK CHECK**: One method of testing a specific component of a plan. Typically, the owner or author of the component reviews it for accuracy and completeness and signs off.
52. **DISASTER**: A sudden, unplanned calamitous event causing great damage or loss. (1) Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time. (2) In the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time. (3) The period when company management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location. *SIMILAR TERMS*: Business Interruption; Outage; Catastrophe.
53. **DISASTER RECOVERY**: Activities and programs designed to return the entity to an acceptable condition. (1) The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.
54. **DISASTER RECOVERY OR BUSINESS CONTINUITY COORDINATOR**: The Disaster Recovery Coordinator may be responsible for overall recovery of an organization or unit(s). SIMILAR TERMS: Business Recovery Coordinator.
55. **DISASTER RECOVERY INSTITUTE INTERNATIONAL** (DRI INTERNATIONAL, www.drii.org): A not-for-profit organization that offers certification and educational offerings for business continuity professionals.
56. **DISASTER RECOVERY PLAN**: The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
57. **DISASTER RECOVERY PLANNING**: The technological aspect of Business Continuity Planning. The advance planning and preparation that is necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster. SIMILAR TERMS: Contingency Planning; Business Resumption Planning; Corporate Contingency Planning; Business Interruption Planning; Disaster Preparedness.
58. **DISASTER RECOVERY SOFTWARE**: An application program developed to assist an organization in writing a comprehensive disaster recovery plan.
59. **DISASTER RECOVERY TEAMS** (Business Recovery Teams): A structured group of teams ready to take control of the recovery operations if a disaster should occur.
60. **ELECTRONIC VAULTING**: Electronically forwarding backup data to an offsite server or storage facility. Vaulting eliminates the need for tape shipment and therefore significantly shortens the time required to move the data offsite.

61. **EMERGENCY**: A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.
62. **EMERGENCY PREPAREDNESS**: The discipline that ensures an organization, or community's readiness to respond to an emergency in a coordinated, timely, and effective manner.
63. **EMERGENCY PROCEDURES**: A plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.
64. **EMERGENCY OPERATIONS CENTER** (EOC): A site from which response teams/officials (municipal, county, state and federal) exercise direction and control in an emergency or disaster.
65. **ENVIRONMENT RESTORATION**: Recreation of the critical business operations in an alternate location, including people, equipment and communications capability.
66. **EXECUTIVE / MANAGEMENT SUCCESSION**: A predetermined plan for ensuring the continuity of authority, decision-making, and communication in the event that key members of senior management suddenly become incapacitated, or in the event that a crisis occurs while key members of senior management are unavailable.
67. **EXERCISE**: An activity that is performed for the purpose of training and conditioning team members, and improving their performance. Types of exercises include: Table Top Exercise, Simulation Exercise, Operational Exercise and Mock Disaster.
68. **FILE SHADOWING**: The asynchronous duplication of the production database on separate media to ensure data availability, currency and accuracy. File shadowing can be used as a disaster recovery solution if performed remotely, to improve both the recovery time and recovery point objectives. *SIMILAR TERMS*: Data Replication, Journaling, Disk Mirroring.
69. **FINANCIAL IMPACT**: An operating expense that continues following an interruption or disaster, which as a result of the event cannot be offset by income and directly affects the financial position of the organization.
70. **FORWARD RECOVERY**: The process of recovering a database to the point of failure by applying active journal or log data to the current backup files of the database.
71. **HAZARD OR THREAT IDENTIFICATION**: The process of identifying situations or conditions that have the potential to cause injury to people, damage to property, or damage to the environment.
72. **HIGH AVAILABILITY**: Systems or applications requiring a very high level of reliability and availability. High availability systems typically operate 24x7 and usually require built in redundancy built-in redundancy to minimize the risk of downtime due to hardware and/or telecommunication failures.
73. **HIGH-RISK AREAS**: Heavily populated areas, particularly susceptible to high-intensity earthquakes, floods, tsunamis or other disasters, for which emergency response may be necessary in the event of a disaster.
74. **HOT SITE**: An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.
75. **HUMAN THREATS**: Possible disruptions in operations resulting from human actions. (i.e., disgruntled employee, terrorism, blackmail, job actions, riots, etc.)
76. **INCIDENT COMMAND SYSTEM** (ICS): Combination of facilities, equipment, personnel, procedures and communications operating within a common organizational

structure with responsibility for management of assigned resources to effectively direct and control the response to an incident. Intended to expand, as situation requires larger resources, without requiring new, reorganized command structure. (NEMA Term)

77. **INCIDENT MANAGER**: Commands the local EOC reporting up to senior management on the recovery progress. Has the authority to invoke the local recovery plan.
78. **INCIDENT RESPONSE**: The response of an organization to a disaster or other significant event that may significantly impact the organization, its people or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.
79. **INTEGRATED TEST**: A test conducted on multiple components of a plan, in conjunction with each other, typically under simulated operating conditions
80. **INTERIM SITE**: A temporary location used to continue performing business functions after vacating a recovery site and before the original or new home site can be occupied. Move to an interim site may be necessary if ongoing stay at the recovery site is not feasible for the period of time needed or if the recovery site is located far from the normal business site that was impacted by the disaster. An interim site move is planned and scheduled in advance to minimize disruption of business processes; equal care must be given to transferring critical functions from the interim site back to the normal business site.
81. **INTERNAL HOT SITE**: A fully equipped alternate processing site owned and operated by the organization.
82. **JOURNALING**: The process of logging changes or updates to a database since the last full backup. Journals can be used to recover previous versions of a file before updates were made, or to facilitate disaster recovery, if performed remotely, by applying changes to the last safe backup. *SIMILAR TERMS*: File Shadowing, Data Replication, Disk Mirroring.
83. **LAN RECOVERY**: The component of business continuity that deals specifically with the replacement of LAN equipment and the restoration of essential data and software in the event of a disaster. *SIMILAR TERM*: Client/Server Recovery.
84. **LINE REROUTING**: A short-term change in the routing of telephone traffic, which can be planned and recurring, or a reaction to an outage situation. Many regional telephone companies offer service that allows a computer center to quickly reroute a network of dedicated lines to a backup site.
85. **LOSS REDUCTION**: The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction involves planning for, and reacting to, an event to limit its impact. Examples of loss reduction include sprinkler systems, insurance policies and evacuation procedures.
86. **LOST TRANSACTION RECOVERY**: Recovery of data (paper within the work area and/or system entries) destroyed or lost at the time of the disaster or interruption. Paper documents may need to be requested or re-acquired from original sources. Data for system entries may need to be recreated or reentered.
87. **MISSION-CRITICAL APPLICATION**: An application that is essential to the organization’s ability to perform necessary business functions. Loss of the mission-critical application would have a negative impact on the business, as well as legal or regulatory impacts.

88. **MOBILE RECOVERY**: A mobilized resource purchased or contracted for the purpose of business recovery. The mobile recovery center might include: computers, workstations, telephone, electrical power, etc.
89. **MOCK DISASTER**: One method of exercising teams in which participants are challenged to determine the actions they would take in the event of a specific disaster scenario. Mock disasters usually involve all, or most, of the applicable teams. Under the guidance of exercise coordinators, the teams walk through the actions they would take per their plans, or simulate performance of these actions. Teams may be at a single exercise location, or at multiple locations, with communication between teams simulating actual 'disaster mode' communications. A mock disaster will typically operate on a compressed timeframe representing many hours, or even days.
90. **NATURAL THREATS**: Events caused by nature that have the potential to impact an organization.
91. **NETWORK OUTAGE**: An interruption in system availability resulting from a communication failure affecting a network of computer terminals, processors and/or workstations.
92. **OFF-SITE STORAGE**: Alternate facility, other than the primary production site, where duplicated vital records and documentation may be stored for use during disaster recovery.
93. **OPERATIONAL EXERCISE**: One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Operational exercises, which may involve one or more teams, are typically performed under actual operating conditions at the designated alternate location, using the specific recovery configuration that would be available in a disaster.
94. **OPERATIONAL IMPACT ANALYSIS**: Determines the impact of the loss of an operational or technological resource. The loss of a system, network or other critical resource may affect a number of business processes.
95. **OPERATIONAL TEST**: A test conducted on one or more components of a plan under actual operating conditions.
96. **PLAN ADMINISTRATOR**: The individual responsible for documenting recovery activities and tracking recovery progress.
97. **PEER REVIEW**: One method of testing a specific component of a plan. Typically, the component is reviewed for accuracy and completeness by personnel (other than the owner or author) with appropriate technical or business knowledge.
98. **PLAN MAINTENANCE PROCEDURES**: Maintenance procedures outline the process for the review and update of business continuity plans.
99. **RECIPROCAL AGREEMENT**: Agreement between two organizations (or two internal business groups) with basically the same equipment/same environment that allows each one to recover at each other's site.
100. **RECOVERY**: Process of planning for and/or implementing expanded operations to address less time-sensitive business operations immediately following an interruption or disaster. 1) The start of the actual process or function that uses the restored technology and location.
101. **RECOVERY PERIOD**: The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.

102. **RECOVERY SERVICES CONTRACT**: A contract with an external organization guaranteeing the provision of specified equipment, facilities, or services, usually within a specified time period, in the event of a business interruption. A typical contract will specify a monthly subscription fee, a declaration fee, usage costs, method and amount of testing, termination options, penalties and liabilities, etc.
103. **RECOVERY STRATEGY**: An approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major outage. Plans and methodologies are determined by the organizations strategy. There may be more than one methodology or solution for an organizations strategy. Examples of methodologies and solutions include, contracting for Hot-site or Cold-site, building an internal Hot-site or Cold-site, identifying an Alternate Work Area, a Consortium or Reciprocal Agreement, contracting for Mobile Recovery or Crate and Ship, and many others.
104. **RECOVERY POINT OBJECTIVE** (RPO): The point in time to which systems and data must be recovered after an outage (e.g. end of previous day's processing). RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the systems or functions have been recovered.
105. **RECOVERY TIME OBJECTIVE** (RTO): The period of time within which systems, applications or functions must be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. *SIMILAR TERMS*: Maximum Allowable Downtime.
106. **RESPONSE**: The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety and evacuation, Response also addresses the policies, procedures and actions to be followed in the event of an emergency. 1) The step or stage that immediately follows a disaster event where actions begin as a result of the event having occurred. *SIMILAR TERMS*: Emergency Response, Disaster Response, Immediate Response and Damage Assessment.
107. **RESTORATION**: Process of planning for and/or implementing procedures for the repair or relocation of the primary site and its contents, and for the restoration of normal operations at the primary site.
108. **RESUMPTION**: The process of planning for and/or implementing the restarting of defined business operations following a disaster, usually beginning with the most critical or time-sensitive functions and continuing along a planned sequence to address all identified areas required by the business. (1) The step or stage after the impacted infrastructure, data, communications and environment has been successfully reestablished at an alternate location.
109. **RISK**: Potential for exposure to loss. Risks, either man-made or natural, are constant. The potential is usually measured by its probability in years.
110. **RISK ASSESSMENT / ANALYSIS**: Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

111. **RISK MITIGATION**: Implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner.
112. **SALVAGE & RESTORATION**: The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc. following a disaster.
113. **SIMULATION EXERCISE**: One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises, which may involve one or more teams, are performed under conditions that at least partially simulate 'disaster mode.' They may or may not be performed at the designated alternate location, and typically use only a partial recovery configuration.
114. **STANDALONE TEST**: A test conducted on a specific component of a plan, in isolation from other components, typically under simulated operating conditions.
115. **STRUCTURED WALKTHROUGH**: One method of testing a specific component of a plan. Typically, a team member makes a detailed presentation of the component to other team members (and possibly non-members) for their critique and evaluation.
116. **SUBSCRIPTION**: Contract commitment that provides an organization with the right to utilize a vendor recovery facility for processing capability in the event of a disaster declaration.
117. **SYSTEM DOWNTIME**: A planned or unplanned interruption in system availability.
118. **TABLE TOP EXERCISE**: One method of exercising teams in which participants review and discuss the actions they would take per their plans, but do not perform any of these actions. The exercise can be conducted with a single team, or multiple teams, typically under the guidance of exercise facilitators.
119. **TEST**: An activity that is performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Types of tests include: Desk Check, Peer Review, Structured Walkthrough, Standalone Test, Integrated Test, and Operational Test.
120. **TEST PLAN**: A document designed to periodically exercise specific action tasks and procedures to ensure viability in a real disaster or severe outage situation.
121. **UNINTERRUPTIBLE POWER SUPPLY** (UPS): A backup supply that provides continuous power to critical equipment in the event that commercial power is lost.
122. **VITAL RECORD**: A record that must be preserved and available for retrieval if needed.
123. **WARM SITE**: An alternate processing site, which is equipped with some hardware, and communications interfaces, electrical and environmental conditioning that is only capable of providing backup after additional provisioning, software or customization, is performed.
124. **WORKAROUND PROCEDURES**: Interim procedures that may be used by a business unit to enable it to continue to perform its critical functions during temporary unavailability of specific application systems, electronic or hard copy data, voice or data communication systems, specialized equipment, office facilities, personnel, or external services. *SIMILAR TERMS*: Interim Contingencies.

Links to a number of other Business Continuity and related glossaries may be found at http://www.rothstein.com/links/links.html under the sub-heading "Glossaries."